13-05-2026

Kandidatspeciale

Relativ vs. Absolut vurdering af personoplysningsbegrebet

Statistik:	
Sider	74
Ord	20.717
Tegn (uden mellemrum)	123.421
Tegn (med mellemrum)	143.993
Afsnit	410
Linjer	2.142

☐ Medtag tekstfelter, fodnoter og slutnoter

Udarbejdet af: Cecilie Laura Olesen (20214600) og Mathias Friis Vestergaard (20215018)
VEJLEDER: TANJA KAMMERSGAARD CHRISTENSEN
UDDANNELSESSTED: AALBORG UNIVERSITET

1. Abstract

Through this project the question of whether personal data should be interpreted through a relative or absolute assessment has been asked and answered. This question has been asked and answered because the assessment is an essential part of the General Data Protection Regulation (GDPR).
As a means for answering this question the legal dogmatic method has been used. This method has been chosen because of its strength regarding analyzing an area of law.

Throughout the project there has been a focus on the GDPR and its legal definition of personal data and recital 26 in GDPR. Furthermore, the project has analyzed four Court Justice European Union (hereafter CJEU) cases because case law is an important part of interpreting applicable law. These four cases have helped answer the question of which assessment is the correct one. Through these analyses it has become clear that the CJEU uses the relative assessment, which indicates that this is the correct assessment when interpreting personal data as a concept.

Besides analyzing CJEU cases the project has also analyzed three supervisory authority's decisions. These decisions have been analyzed to see whether the supervisory authorities use the correct assessment as established by CJEU. Through these analyses it is clear that not every supervisory authority uses the relative assessment regarding personal data.

Furthermore, the project has analyzed the proposed change to the legal definition of personal data from The Digital Omnibus (Omnibus). This analysis is relevant because a change in the legal definition would mean that the field of application of GDPR would change. The analysis has shown that the proposed change would have severe negative effects and it should therefore not be adopted.

Indhold

2. Indledning

I EU er der reguleringer for at sikre, at samarbejdet mellem medlemslandene har den samme beskyttelse og de samme muligheder på mange områder på tværs af landegrænser. Dette er ikke anderledes for området omhandlende databeskyttelse. I EU er der nogle fundamentale rettigheder, som sikres gennem chartret, hvoraf en af disse er retten til beskyttelse af personoplysninger, der dækkes af artikel 8.[1]

Beskyttelsen af personoplysninger er dermed en central og grundlæggende rettighed i EU, som der skal værnes om. På baggrund af artikel 8 i chartret, blev der d. 27. april i 2016 vedtaget en forordning, der har til formål at sikre, at denne grundlæggende rettighed blev og forbliver sikret, samt beskrive hvordan medlemslandene skal varetage denne opgave. Forordningen *Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF* fik fuld virkning i maj, 2018 og er den forordning, vi i dag kender under navnet kort kaldet databeskyttelsesforordningen eller GDPR.[2]

Databeskyttelsesforordningen har fastlagt reglerne for, hvordan der behandles personoplysninger i EU eller behandles personoplysninger omhandlende EU-borger, og hvilke krav der er til sikkerhed, indsamling osv. For at kunne overholde databeskyttelsesforordningen eller anden databeskyttelsesretlig regulering, herunder f.eks.. databeskyttelsesloven, er det centralt at vide, hvad der reguleres, herunder anvendelsesområdet. Det er med andre ord vigtigt at forstå, hvad en personoplysning er, da det er det eneste område databeskyttelsesforordningen dækker.[3]

Personoplysninger som begreb er et område hvori, der er blevet forsket af mange forskere, og det er også tidligere blevet undersøgt, hvordan begrebet personoplysning skal forstås, samt

[1] DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER
[2] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679
[3] Ibid.

hvornår en personoplysning går fra at være en personoplysning, til ikke at være en personoplysning længere eller omvendt.[4]

Spørgsmålet om hvornår noget er en personoplysning er et essentielt spørgsmål, idet baggrunden for EU-regulering er at skabe ensartethed i hele Unionen og dermed sikre, at alle borgere og selskaber i EU har de samme muligheder og nyder den samme beskyttelse. Det er derfor vigtigt, at området er klarlagt, da spørgsmålet er essentielt i forhold til, hvilken beskyttelse oplysninger skal være underlagt.
Samarbejde og lighed i forhold til reglerne i EU udspringer fra Lissabon-traktaten. Traktaten gør det klart, at baggrunden for den Europæiske Union er at fremme de samme værdier og skabe et solidt og stærkt indre marked, for at fremme EU-medlemslandene og dets borgere.[5]

For at sikre, at borgerne på tværs af medlemslandene har de samme rettigheder og beskyttelse, er det vigtigt at medlemslandene behandler og fortolker de grundlæggende rettigheder så ensartet som muligt. Med fokus på databeskyttelse er det dermed essentielt, at medlemslandene forstår personoplysningsbegrebet ens og behandler personoplysninger på samme måde.

I forbindelse med ikrafttrædelsen af forordningen er det krævet i databeskyttelsesforordningens artikel 51, at medlemslandene opretter en uafhængig offentlig tilsynsmyndighed. Artikel 51 stk. 2. 1. led lyder således: "*Hver enkelt tilsynsmyndighed bidrager til ensartet anvendelse af denne forordning i hele Unionen".* Det kan dermed ses, at tilsynsmyndighederne har et ansvar for at sikre sig, at medlemslandene anvender og fortolker databeskyttelsesforordningen på samme måde.[6]

Det er derfor vigtigt at forstå, hvordan personoplysninger skal forstås og defineres, samt om vurderingen, der laves i forhold til disse, skal være en relativ eller absolut vurdering. Betydningen af relativ og absolut vurdering vil blive gennemgået senere i specialet.
Hver tilsynsmyndighed har jurisdiktion over egne nationale afgørelser vedrørende brud på databeskyttelsesreglerne og ved at gennemgå tidligere administrative afgørelser, kan det

[4] Personoplysningsbegrebet i GDPR (Andersen, 2025)
[5] LISSABONTRAKTATEN OM ÆNDRING AF TRAKTATEN OM DEN EUROPÆISKE UNION OG TRAKTATEN OM OPRETTELSE AF DET EUROPÆISKE FÆLLESKAB (2007/C306/01)
[6] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679

klarlægges, hvilken vurdering forskellige tilsynsmyndigheder lægger vægt på. En eventuel forskel på hvordan vurderingen af personoplysninger foretages kan skabe problemer for databehandlinger, der bevæger sig på tværs af landegrænser. Dette kan skade beskyttelsen af de registrerede og besværliggøre processen for de dataansvarlige.

Det ses dermed relevant at få undersøgt, hvilken af disse tilgange, der kan anses for at være den korrekte i vurderingen af begrebet *personoplysninger*, hvilket denne opgave vil gå i dybden med på baggrund af EU-domstolens afgørelser, tilsynsmyndigheders afgørelser, tidligere forskning i området og lovgivning, som den lyder i dag.

Der vil også blive undersøgt, hvordan fremtidig lovgivning vil kunne få betydning for området. Dette gøres ved at se på lovforslaget Den Digitale Omnibus og undersøge, hvilken betydning dette lovforslag vil have for personoplysningsbegrebet og fortolkningen af dette.

3. Problemstilling

Der vil i specialet blive arbejdet ud fra problemstillingen:

Skal vurderingen af, om der er tale om personoplysninger, vurderet efter databeskyttelsesforordningens definition af personoplysninger, tilsynsmyndigheders afgørelser og EU-domstolens fortolkning heraf, bero på en relativ eller absolut vurdering. Hvad kan der udledes herom af databeskyttelsesreglerne, afgørelser fra tilsynsmyndigheder, retspraksis fra EU-domstolene, samt lovforslaget om den digitale omnibus og dennes betydning for gældende ret på området.

4. Afgrænsning

Det vil i følgende afsnit blive beskrevet, hvordan specialets område er blevet afgrænset, for at kunne besvare problemformuleringen.

Specialet undersøger, hvordan personoplysningsbegrebet i databeskyttelsesforordningen skal fortolkes i forhold til en relativ eller absolut vurdering. Specialet afgrænses derfor til kun at omhandle databeskyttelsesforordningen. Specialet tager udgangspunkt i databeskyttelsesforordningens artikler, herunder med fokus på art. 4, stk. 1., samt databeskyttelsesforordningens betragtninger, herunder primært betragtning 26.

I specialet fokuseres der udelukkende på området inden for EU/EØS, hvorfor der ikke vil blive arbejdet med tredjelandsoverførsler.

Flere særlove indeholder regler omkring databeskyttelse, hvori personoplysningsbegrebet kan være relevant, herunder f.eks.. sundhedsloven, men eftersom legaldefinitionen for personoplysningbegrebet findes i databeskyttelsesforordningen, afgrænses specialet til kun at behandle denne. Der behandles derfor ikke særlovgivning i specialet.

Ydermere vil der i specialet blive analyseret domme fra EU-domstolen samt afgørelser fra tilsynsmyndigheder i EU, hvori der tages stilling til databeskyttelsesretlige spørgsmål. I de tilfælde, hvor dommene omhandler anden lovgivning end databeskyttelsesforordningen, vil denne anden lovgivning ikke blive behandlet i specialet. I tilfælde hvor der i dommene eller afgørelserne behandles databeskyttelsesretlige spørgsmål, som ikke er direkte relevante for specialets problemformulering, vil disse spørgsmål heller ikke blive behandlet.

5. Metodeafsnit

Det vil i følgende afsnit blive beskrevet, med hvilken metode specialets problemformulering vil blive besvaret, samt hvilke overvejelser, der er gjort i specialet med hensyn til metode. Det vil blive beskrevet, hvordan den juridiske metode anvendes i specialet, og hvilke retskilder, der anvendes til både teori, analyse og diskussion. Den følgende beskrivelse af specialets metode beskriver dermed, hvordan gældende ret er udledt i specialet.

For at besvare specialets problemformulering, vil der i specialet blive anvendt juridisk metode. Juridisk metode anvendes til at beskrive, analysere og systematisere et retsområde, for at undersøge, hvad gældende ret er på området.[7] I forbindelse med den juridiske metode er det relevant at vurdere pålideligheden og retskildeværdien af de kilder, der anvendes når gældende ret skal udledes.[8] Juridisk metode vil blive anvendt af den årsag, at formålet med specialet er at finde frem til gældende ret inden for Databeskyttelsesret, i forbindelse med personoplysningsbegrebet og dets beskrivelse samt anvendelse i EU-retligt perspektiv.

Besvarelsen af problemformuleringen i dette speciale indeholder en analyse med flere forskellige retskilder, herunder anvendes national ret og EU-ret. Specialets analyse vil tage udgangspunkt i love og retsregler, da disse har den højeste retskildeværdi.[9] Der vil i specialet være særligt fokus på databeskyttelsesforordningen, der udspringer fra EU-Kommissionen. Forordninger er gældende ret i alle medlemslande, og disse skal ikke implementeres i national ret på samme måde, som direktiver skal.[10] Databeskyttelsesforordningen er derfor både national ret og EU-ret, da den som forordning også er gældende for medlemslandene. Tilgangen til disse forskellige retskilder vil være et fokus på EU-retten, eftersom problemstillingen i specialet lægger op til at finde gældende ret og anvendelse af personoplysningsbegrebet i henhold til relativ og absolut vurdering generelt i EU, som en samlet Union, og ikke de enkelte nationer alene, samt fordi begrebet personoplysninger udspringer af EU-lovgivning.

[7] Retsvidenskabsteori (Munk-Hansen, 2018, s. 193)
[8] Juraens verden (Hamer & Schaumburg-Müller, 2020, s. 19)
[9] Ibid. s. 19, 67-69
[10] EU's love (Folketinget, u.d.)

Der vil blive lagt vægt på databeskyttelsesforordningens artikler samt formålet med databeskyttelsesforordningen. Ydermere vil der blive inddraget retspraksis i form af afgørelser fra EU-domstolen på området.

Databeskyttelsesforordningen vil igennem specialet blive fortolket gennem både en ordlydsfortolkning og formålsfortolkning. Ved en ordlydsfortolkning lægges der vægt på ordvalget i retsreglerne, og retsreglerne fortolkes ud fra den generelle forståelse af ordvalget.[11] Eftersom databeskyttelsesforordningen er en EU-retlig kilde, skal der ved ordlydsfortolkningen tages hensyn til, at EU-retlige kilder er affattet på mange forskellige sprog.[12] Formuleringerne ses som autentiske, hvorfor der i teorien ikke burde være forskel på ordlydsfortolkning, uanset hvilket sprog fortolkningen laves ud fra. I praksis kan der dog være små forskelle, hvorfor fortolkningen i princippet bør laves ud fra samtlige oversættelser. Dette ses dog ikke proportionalt med specialets omfang, hvorfor ordlydsfortolkningen kun vil tage udgangspunkt i den danske version af databeskyttelsesforordningen.
Ved en formålsfortolkning fortolkes retsreglerne ud fra hensigten og formålet med disse retsregler. Ved en formålsfortolkning sikres det, at retsreglerne ikke bliver fortolket i strid med deres hensigt og formål.[13] Databeskyttelsesforordningen vil derfor også blive fortolket ud fra dens hensigt og formål, som er at finde i forordningens betragtninger.

Specialet vil derudover inddrage flere EU-domme for at undersøge, hvordan EU-domstolen i praksis har vurderet kravene for, at der er tale om personoplysninger. EU-domstolens afgørelser har den højeste retskildeværdi, når det kommer til fortolkning af EU-retten ud fra retspraksis. Den højeste retsinstans, man kan rette appel afgørelser til, indenfor EU-retten, er EU-domstolen, og de har dermed det sidste ord i fortolkningen af EU-lovgivning.[14] Domme og afgørelse er anset som en vigtig retskildegruppe, da lignede sager helst skulle afgøres på samme måde.[15] I forhold til retskildeværdien af en dom eller afgørelse er det herunder også relevant at have med i vurderingen, hvilken retsinstans der har afsagt dommen. Dette skyldes, at f.eks.. landsretsdomme i Danmark kan underkendes af højesteret, eller at Datatilsynets

[11] Den juridiske metode - en introduktion (Hansen & Werlauff, 2002, s. 175)
[12] Sprog (Den europæiske union, u.d.)
[13] Juraens verden (Hamer & Schaumburg-Müller, 2020, s. 74-75)
[14] Ibid. s. 155-156
[15] Ibid. s. 21

afgørelser kan underkendes af EU-domstolene.[16] Det er derfor relevant for værdien af dommen eller afgørelsen, hvilken retsinstans der afsiger denne.

Der vil i specialet blive lagt fokus på dommen C-582/14 *Patrick Breyer v Bundesrepublik Deutschland (herefter kaldet Breyer-dommen).* Dommen vil være med til at give et indblik i, hvad der skal til for, at data bliver til personoplysninger, samt give et billede af de overvejelser, domstolen gør sig for at vurdere, om data er personoplysninger. Der vil også blive lagt vægt på *C-434/16 Peter Nowak v Data Protection Commissioner (Herefter kalder Nowak-dommen)* da denne dom viser, hvor langt personoplysningsbegrebet strækker sig, samt at begrebet personoplysninger også omhandler perifere oplysninger, der kan relatere sig til en fysisk person. Dommen *C-604/22 IAB Europe* vil også blive inddraget i specialet i forbindelse med analysen af, hvordan EU-domstolen vurderer personoplysninger, da dommen går direkte ind og diskuterer, hvor fokus skal ligge, når vurderingen af, hvorvidt identifikation er mulig, skal foretages. Dette er den første EU-dom, i dette speciale, der er behandlet efter databeskyttelsesforordningens implementering og kan dermed give et indblik i om vurderingen har ændret sig i forbindelse med implementering af databeskyttelsesforordningen, eller om den følger den tidligere retspraksis fra EU-domstolen. Der vil også blive analyseret på dommen *C-413/23 SRB v EDPS (Herefter kaldet SRB-dommen)* **-** da afgørelsen giver et godt indblik i, hvor strengt EU-domstolen vurderer spørgsmålet, om hvornår en oplysning er en personoplysning for en modtager. Dommene vil tilsammen give et indblik i, hvordan EU-domstolen fortolker personoplysningsbegrebet og vurderingen af dette begreb. Breyer-dommen er relevant for undersøgelsesområdet, og denne er udvalgt ud fra, at vores undersøgelsesområde udspringer fra denne dom og diskussionen i sagen, omkring hvilken af de to vurderingsmetoder, der skal anses for at være den korrekte. De tre resterende domme er fundet gennem en generel undersøgelse af retsområdet, idet det er store sager, der skabte røre i den databeskyttelsesretlige verden.

Medlemslandene i EU har deres egen tilsynsmyndighed til at sikre kontrol med databeskyttelsesforordningen, samt generel overholdelse af databeskyttelse.[17] Tilsynsmyndighederne har til opgave blandt andet, at føre tilsyn med og håndhæve

[16] Ibid. s. 22
[17] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679, artikel 52

databeskyttelsesforordningen, og til at sikre dette formål har de visse beføjelser, herunder f.eks. mulighed for at udstede advarsler, samt indstille til bøder eller udtale kritik af en dataansvarlig eller databehandler.[18] Nogle af tilsynsmyndighedernes afgørelser offentliggøres, da dette kan være med til at udlede retspraksis på området samt skabe bevidsthed på området.[19] Tilsynsmyndighederne er ikke direkte forbundne med EU, hvorfor disse ikke nødvendigvis fortolker databeskyttelsesforordningen ens med hinanden og/eller med EU-domstolen. I forbindelse med udledelsen af gældende ret, vil det derfor blive undersøgt, hvordan og hvor disse tilsynsmyndigheder fortolker databeskyttelsesforordningen forskelligt herunder med fokus på personoplysningsbegrebet og vurdering af, hvorvidt dette anvendes relativ eller absolut. Dette vil blive gjort ud fra tilsynsmyndighedernes afgørelser. Flere af tilsynsmyndighederne offentliggør kun deres afgørelser på deres nationale sprog, hvorfor det har været nødvendigt at oversætte disse afgørelser. Afgørelserne er oversat til dansk ved brug af Deepl, og der tages her forbehold for mindre fejl i forbindelse med oversættelsen.

Tilsynsmyndighedernes afgørelser vil i forbindelse med udledningen af gældende ret, ikke blive anvendt med samme retskildeværdi som EU-domstolens retspraksis. Det skyldes, at administrative afgørelser, som tilsynsmyndighedernes afgørelser er, ikke kan tillægges samme retskildeværdi som EU-domstolens retspraksis, da disse afgørelser altid kan underkendes af EU-domstolen.[20] Disse administrative afgørelser kan dog være et værktøj til at se, hvordan databeskyttelsesforordningen skal fortolkes ifølge tilsynsmyndighederne. Hvis man benytter administrative afgørelser til at fortolke databeskyttelsesforordningen, skal man dog have for øje, at andre medlemslandes tilsynsmyndigheders afgørelser ikke har direkte anvendelse på den danske retsstilling i forhold til databeskyttelsesforordningen. Dette skyldes, at disse ses som fremmedret, og derfor ikke har betydning for retsstillingen i Danmark. Afgørelserne kan dog være med til at illustrere fortolkningen af forskellige problemstillinger, som kan anvendes supplerende til den danske tilsynsmyndigheds vurderinger. [21]

Senioradvokat og ph.d.- Stipendiat Kasper Bjerre Hendrup Andersen er, i artiklen "*En fælles databeskyttelsesret?",* kommet frem til, at øvrige medlemslandenes doms- og administrative praksis bør anses som et muligt fortolkningsbidrag. Han åbner dermed op for muligheden for

[18] Ibid. artikel 57 & 58
[19] Afgørelser (Datatilsynet u.d.)
[20] Danske Retskilder: Retsafgørelser (retspraksis)(CBS Library & academic services, u.d.)
[21] Persondatarettens kilder og metode (Blume, 2020, s. 73)

at anvende øvrige medlemslandenes domme og administrative afgørelser som fortolkningsbidrag. Et lignende synspunkt ses ved Peter Blume i *Persondatarettens kilder og metode*, hvori han mener, at øvrige medlemslandes domme bør kunne anvendes som fortolkningsbidrag.[22]
Der er til analysen udvalgt en tilsynsmyndighedsafgørelse fra hver især Danmark, Spanien og Frankrig. Den danske tilsynsmyndighedsafgørelse er valgt, da denne juridisk er mest relevant for os i Danmark, hvorfor denne også vil blive analyseret først. Derudover er de andre to afgørelser valgt for at undersøge, hvordan tilsynsmyndighederne i andre EU-lande vurderer personoplysningsbegrebet. I forbindelse med udvælgelsen af afgørelser, har specialet været lidt begrænset, da ikke alle tilsynsmyndigheder offentliggører alle (eller mange) af deres afgørelser.

Der vil i specialet også blive anvendt udtalelser fra European Data Protection Board (EDPB) og European Data Protection Supervisor (EDPS). EDPB's opgaver består i foruden at komme med vejledninger omkring forståelse og fortolkning af databeskyttelsesforordningen, også at komme med bindende afgørelse i visse tilfælde. Disse tilfælde er særligt ved grænseoverskridende behandling.[23]
EDPS er EU's uafhængige tilsynsmyndighed, og deres opgaver består i, at overvåge og rådgive EU institutioner og organer i forbindelse med behandling af personoplysninger.[24]
Eftersom begge organer har til opgave at rådgive omkring fortolkning af Databeskyttelsesforordningen, har udtalelser fra disse organer en vis retskildeværdi.
Foruden udtalelser fra EDPB og EDPS vil specialet også anvende udtalelser fra den tidligere artikel 29-gruppe. Artikel 29-gruppen var en arbejdsgruppe, som blev nedsat ved direktiv 95/46/EF til at behandle spørgsmål omkring privatlivets fred og personoplysninger. Artikel 29-gruppen blev ved ikrafttrædelsen af databeskyttelsesforordningen erstattet af EDPB.[25]
Denne tidligere arbejdsgruppes udtalelser har også en vis retskildeværdi, da denne blev nedsat netop med formålet at besvare spørgsmål omkring personoplysninger.

[22] Ibid.
[23] Role of the EDPB (European Data Protection Board, u.d.)
[24] About us (European Data Protection supervisor, u.d.)
[25] Arv: Artikel 29-gruppen (EDPB, u.d.)

I dette speciale vil der blandt andet blive gjort brug af relevant juridisk litteratur, herunder blandt andet Kristian Korfits Nielsen & Anders Lotterup's *Databeskyttelsesforordningen og databeskyttelsesloven* og Henrik Udsen & David Knobel's *Introduktion til Databeskyttelsesret.* Ydermere vil Kasper Bjerre Hendrup Andersen's ph.d.-afhandling *Personoplysningsbegrebet i GDPR* også blive anvendt. Den udvalgte juridisk litteratur anvendes for at opnå en dybere forståelse af databeskyttelsesret. Juridisk litteratur har ikke nogen retskildeværdi, dog kan litteraturen være god til at skabe en dybere forståelse af emnet. Dette er særligt relevant, hvis den juridiske litteratur er resultatet af en kyndig og nøje analyse af retsregler og afgørelser.[26]

Ydermere vil der i specialet også blive kigget ind i lovforslaget om Den Digitale Omnibus i forhold til de lovændringer forslaget vil få for databeskyttelsesforordningen, samt den generelle anvendelse af denne, hvis dette vedtages, herunder specifikt i forhold til en evt. ændring i personoplysningsbegrebet.[27]
Lovforslaget har ingen retskildeværdi, da det endnu ikke er vedtaget, hvorfor det heller ikke anvendes til at udlede gældende ret, men derimod for at undersøge, hvilken betydning en evt. vedtagelse vil få for gældende ret.

[26] Persondatarettens kilder og metode (Blume, P., 2020, s. 55)
[27] Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om ændring af forordning (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 og direktiv 2002/58/EF, (EU) 2022/2555 og (EU) 2022/2557 for så vidt angår forenkling af det digitale regelsæt og om ophævelse af forordning (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 og direktiv (EU) 2019/1024 (den digitale omnibus)

6. Teoriafsnit

For at kunne besvare specialets problemformulering, er der teori på området, som det ses relevant at gennemgå inden, der analyseres EU-domme og tilsynsmyndighedsafgørelser. Specialet vil derfor i de efterfølgende afsnit gennemgå formålet og baggrund for databeskyttelsesforordningen, da det er denne analyserne, foretages ud fra, hvorfor det ses relevant at have formålet for øje. Derudover vil legaldefinitionen af personoplysninger blive gennemgået, da det er ud fra denne legal definition, at specialet forsøger at besvare problemformuleringen. Ydermere vil teorien bag absolut og relativ vurdering også blive gennemgået, idet disse teorier er essentielle for analysen og besvarelsen af problemformuleringen.
Derudover ses det også relevant at gennemgå begreberne pseudonymisering og anonymisering, da disse også er relevante begreber i forhold til analysen.
Til sidst i teoriafsnittet kommer der et afsnit omkring tilsynsmyndigheder, og hvorfor disses afgørelser kan være relevante at undersøge i forhold til gældende ret på området, samt i forhold til specialets problemformulering.

6.1. Formålet og baggrund for databeskyttelsesforordningen

Databeskyttelsesforordningen blev vedtaget d. 27. april 2016, og forordningen skulle anvendes fra d. 25. maj 2018.[28] Før databeskyttelsesforordningen blev vedtaget og trådte i kraft, var det Europa Parlamentet og Rådets Direktiv 95/46/EF *om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådan oplysninger*, der var gældende på området. Direktivet var i Danmark implementeret igennem Persondataloven.
Der har været regulering omkring beskyttelse af danskernes personoplysninger helt tilbage til 1979 ved *Lov om offentlige myndigheders registre og lov om private registre.* Behovet for

[28] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679, art. 99.

denne lov kom som følge af danskernes frygt for, at deres personoplysninger vil blive misbrugt i forbindelse med den stigende brug af elektronisk behandling.[29]

Databeskyttelsesforordningen tager afsats i en grundlæggende rettighed i Den Europæiske Unions Charter om Grundlæggende Rettigheder (Chartret). Den grundlæggende rettighed, som databeskyttelsen tager afsats i, er retten til beskyttelse af personoplysninger. Retten til beskyttelse af personoplysninger, der vedrører en selv, findes også i art. 16, stk. 1. i traktaten om Den Europæiske Unions funktionsmåde (TEUF).[30]

Retten til beskyttelse af personoplysninger, er dog ikke en absolut ret, hvilket også følger af databeskyttelsesforordningens betragtning 4. Retten til beskyttelse af personoplysninger skal altid ses i sammenhæng med andre grundlæggende rettigheder, og personoplysningernes funktion i samfundet, samt i overensstemmelse med proportionalitetsprincippet.[31]

Databeskyttelsesforordningen blev set som nødvendig for at sikre samme niveau af beskyttelse af EU-borgernes personoplysninger. Dette skyldes blandt andet, at forskellene i beskyttelsesniveauet fungerede som en hindring for det indre marked.[32]

Netop det indre marked har haft stor betydning for væksten i bevægelserne af personoplysninger på tværs af landegrænserne. Sammen med den teknologiske udvikling har det indre marked øget væksten i mængden af indsamling og behandling både generelt og på tværs af landegrænser.[33]

Det var ud fra denne udvikling, at man så et behov for en stærk og sammenhængende beskyttelsesramme inden for EU.[34]

Formålet med databeskyttelsesforordningen er dermed at beskytte EU-borgernes grundlæggende rettighed til beskyttelse af personoplysninger, men denne skal stadig ses i

[29] Historien om databeskyttelse (Datatilsynet, u.d.)
[30] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 , betragtning 1.
[31] Ibid, betragtning 4.
[32] Ibid, betragtning 9 og 13
[33] Ibid, betragtning 5-6.
[34] Ibid, betragtning 7.

sammenhæng med, og fortolkes ud fra, andre grundlæggende rettigheder, personoplysningernes funktion og proportionalitetsprincippet.

6.2. Hvad er en personoplysning?

Ifølge databeskyttelsesforordningens art. 2, stk. 1. om forordningens materiale anvendelsesområde, finder databeskyttelsesforordningen kun anvendelse, hvis der sker en behandling af personoplysninger. Databeskyttelsesforordningen er derfor ikke relevant, hvis den/de oplysninger, der behandles, ikke er personoplysninger, hvorfor det ses relevant at vurdere, hvorvidt en oplysning er en personoplysning.

Personoplysninger er en legaldefinition i GDPR art. 4, nr. 1. Ordlyden af art. 4, nr. 1. lyder:

"»personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet"

En personoplysning er enhver information om en identificeret eller identificerbar fysisk person. Da alle oplysninger, der kan henføres til en fysisk identificerbar person, er omfattet af begrebet, er der tale om en meget bred definition.
Selvom personen, som oplysningen omhandler, ikke er identificeret, er der stadig tale om en personoplysning, hvis personen er identificerbar.[35] Ved "Identificerbar person" skal forstås, som følge af ordlyden, en fysisk person som kan identificeres enten direkte eller indirekte, herunder f.eks.. ved navn, lokaliseringsdata eller elementer, der er særlige for denne persons fysisk, fysiologiske genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Alle oplysninger, som vil kunne henføres til en person, er omfattet af definitionen, herunder også "uskyldige" informationer som f.eks.. alder og yndlingsfarve.[36]

[35] Databeskyttelsesforordningen og databeskyttelsesloven (Nielsen, & Lotterup, 2025, s. 242)
[36] Introduktion til databeskyttelsesret (Udsen & Knobel, 2026, s. 16)

Så længe personoplysningen kan henføres til en bestemt person, er der tale om personoplysninger. Det er uden betydning, hvilken karakter oplysningen har, for at der er tale om en personoplysning, dog er der flere kategorier indenfor personoplysninger, hvorfor karakteren stadig har en vis relevans, dog ikke for specialets problemformulering.
Hvis personoplysningerne er erstattet af en kode, men det stadig er muligt at føre oplysningen tilbage til den fysiske person, så er der stadig tale om personoplysninger. En oplysning er en personoplysning efter databeskyttelsesforordningens definition, selvom oplysningen først bliver til en personoplysning, når den kombineres med andre oplysninger.[37]

Ordlyden af art. 4, nr. 1, svarer til definitionen på en personoplysning efter den tidligere persondatalovs § 3, nr. 1,[38] som stammede fra Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 *om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*, dog er definitionen i databeskyttelsesforordningen uddybet med en forklaring af begrebet "identificerbar person". Definitionen af personoplysninger er derfor ikke ny i forbindelse med databeskyttelsesforordningen.

På baggrund af forvirringen omkring personoplysningsbegrebet udstedte artikel 29-gruppen en udtalelse omkring personoplysningsbegrebet tilbage i 2007.[39]
Udtalelsen omkring personoplysningsbegrebet er dermed udgivet før databeskyttelsesforordningen blev implementeret, men eftersom definitionen af personoplysninger er den samme, ses udtalelsen stadig relevant for at kunne udlede, hvad der forstås ved *personoplysninger.*
I gruppens udtalelse bliver definitionen opdelt i fire elementer:

- "enhver form for information"
- "om"
- "en identificeret eller identificerbar"
- "fysisk person"[40]

[37] Databeskyttelsesforordningen og databeskyttelsesloven (Nielsen, & Lotterup, 2025, s. 243)
[38] Lov om behandling af personoplysninger, Lov nr 429 af 31/05/2000
[39] Wp29's vejledning nr. 4/2007 af 20. juni 2007 om »begrebet personoplysninger«
[40] Ibid. s. 6

Det første element omkring "enhver form for information" lægger op til en bred fortolkning af hvilke oplysninger, der kan være personoplysninger. Personoplysninger kan derfor både være "objektive" såsom f.eks.. alder, eller "subjektive" herunder f.eks.. udtalelser eller vurderinger. Oplysninger behøver heller ikke at være sande for at være personoplysninger. En personoplysning behøver heller ikke at være en oplysning, der kan skrives ned og opbevares på papir, da f.eks.. lyd og billeddata også kan være personoplysninger.[41]

Det andet element "om" kan give lidt vanskeligheder, da det kan være svært at vurdere, hvornår en (person)oplysning er "om" en person. Generelt vil man mene, at dette er tilfældet, når oplysningen "vedrører" en person. I nogle situationer vil dette være meget ligetil at afgøre. I andre situationer kan en oplysning indirekte omhandle en person, men være tættere knyttet til en genstand f.eks. et hus. I disse situationer kan det være nødvendigt med en analyse af situationen, for at kunne fastlægge, hvorvidt oplysningen er "om" en person.[42]

Det tredje element om "identificeret eller identificerbar" fysisk person giver to muligheder. Hvis en person er identificeret, betyder det, at denne kan skelnes fra andre personer.[43] Denne del af elementet er ofte rimelig ukompliceret, da det er relativt nemt at vurdere, om en person er identificeret. Det kan dog være betydeligt sværere at vurdere, om en person er identificerbar. Med "identificerbar" skal forstås, at personen kan identificeres, men at dette ikke er sket endnu.[44]
Det kan være besværligt at vurdere, hvorvidt en identifikator (oplysning) er nok til at kunne identificere en person, og dette kommer også an på den specifikke situation. I visse situationer skal der flere identifikatorer eller supplerende oplysninger til for, at personen er identificerbar. I betragtning 26 i databeskyttelsesforordningen lægges der vægt på begrebet "identificerbar", da denne siger, at til brug for afgørelsen af om en person kan identificeres skal "[...] alle de hjælpemidler [tages] i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende…".
Hvilket betyder, at det ikke er tilstrækkeligt, at der er en minimal mulighed for at den fysiske person kan identificeres.[45]

[41] Wp29's vejledning nr. 4/2007 af 20. juni 2007 om »begrebet personoplysninger«, s. 6 & 8.
[42] Ibid, s. 9.
[43] Ibid, s 12.
[44] Ibid, s. 12.
[45] Ibid, s. 15.

Dette element er et kompliceret område, og der er mange teoretiske diskussioner omhandlende dette inden for databeskyttelsesområdet. Disse diskussioner er fokusområdet i dette speciale, og der vil derfor blive gået mere i dybden med dette element senere i specialet. Fokus for specialet hviler på diskussionen om, hvilken vurderingsmetode der er den korrekte af absolut og relativ vurdering og disse vil dermed blive gennemgået igennem specialet.

Det fjerde element omkring en "fysisk person" er lidt mere lige til. Databeskyttelsesforordningen finder kun anvendelse på fysiske personer, altså mennesker. Det vil sige, at en oplysning skal omhandle en fysisk person for at være en personoplysning. Dette virker meget lige til, men der kan stadig være situationer, hvor dette bliver lidt kompliceret, f.eks. ved afdøde personer, ufødte børn eller juridiske personer. Ved afdøde personer, kan oplysningerne f.eks. være forbundet med levende fysiske personer på en sådan måde, at disse oplysninger stadig er personoplysninger.[46] Hertil bemærkes, at reglerne i databeskyttelsesforordningen i Danmark finder anvendelse 10 år efter en person er død, jf. databeskyttelsesloven § 2, stk. 5.

Ud fra ovenstående ses det, at det kan være meget kompliceret at vurdere, hvorvidt en oplysning er en personoplysning. Der er gennem tiden blevet afsagt mange EU-domme omkring specifikke oplysninger, og hvorvidt disse er at betragte som personoplysninger, herunder f.eks. C-524/06 *Huber* om registre over udlændinge, C-342/12 *Worten* om arbejdstidsregister, C-73/16 *Puškár* om skatteoplysninger, hvilket også indikerer at det kan være svært, at vurdere hvornår noget er en personoplysning.

6.3. Vurderingen af personoplysninger

Databeskyttelsesområdet har to skoler, som stammer fra tysk teori, inden for vurderingen af begrebet personoplysninger efter databeskyttelsesforordningen artikel 4, herunder den absolutte vurdering og den relative vurdering. De to skoler af tankegange er opdelt ud fra,

[46] Ibid, s. 22.

hvordan det menes, at vurderingen af personoplysninger skal forstås, og i relation til hvem.[47] De to efterfølgende afsnit vil komme ind på baggrunden, betydningen og ideen med de to forskellige vurderinger.

6.3.1 Absolut vurdering

Absolut vurdering er den ene skole af de to teorier. Denne indebærer et meget omfattende synspunkt på, hvornår en oplysning kan kaldes for og kvalificeres som en *personoplysning*. Absolut vurdering af personoplysninger skal forstås således, at hvis noget er personoplysninger, så forbliver det personoplysninger så længe, der er *nogen*, der kan identificere personerne dataene/oplysningerne omhandler, uanset hvem dette er. Dette gør denne vurderingsform til en meget bred og næsten altomspændende vurdering af begrebet personoplysninger. Det er svært at se et reelt scenarie for, hvornår man kommer uden om, at oplysninger "om" en enkeltperson er en personoplysning. Dette syn udspringer fra databeskyttelsesforordningens betragtning 26, der omhandler, hvornår principperne for forordningen skal finde anvendelse, som har ordlyden "[...]bragt i anvendelse af den dataansvarlige eller *en anden person"*.
Det bliver dermed gjort gældende, at vurderingen ikke kun skal foretages ud fra om dataansvarlige kan identificere personen, men også andre personer. Dette lægger baggrunden for vurderingen af personoplysninger i henhold til artikel 4 ud fra denne teori. Det lægger også standarden for, hvornår noget kan ses for at være anonymiseret og dermed ikke dækket af forordningen. Anonymisering vil blive gennemgået mere i dybden senere i specialet.[48]

Det foregående har den betydning, at før man kan vurdere, om en oplysning er en personoplysning, eller om personoplysningerne er anonymiseret, skal enhver persons viden inddrages og tjekkes for at se om der er *nogen*, der vil kunne genkende eller identificere de personer som (person)oplysningerne, der behandles, omhandler.[49]

Fokusset i denne vurdering er dermed blevet lagt på fortolkningen af *"en anden person"*.

[47] Generaladvokatens forslag til afgørelse, *Patrick Breyer v Bundesrepublik Deutschland* (2016, pr. 52)
[48] Ibid. pr. 64 og 65
[49] Personoplysningsbegrebet i GDPR (Andersen, 2025, s. 207)

Denne vurdering har den konsekvens, at databeskyttelsesforordningen vil finde anvendelse på næsten alt databehandling, hvor der i processen har indgået personoplysninger af en eller anden grad. Man skal dermed kigge på hele databehandlerkæden, når man vurderer personoplysningsbegrebet. Denne vurderingsform betyder, at oplysninger oftere vil nyde beskyttelse under databeskyttelsesforordningen, eftersom der næsten altid vil være mulighed for, at der er en tredjemand, der kan identificere enkeltpersoner. Denne fortolkning vil sikre en højere beskyttelse af borgerne i EU, men vil besværliggøre databehandling for selskaber o.lign i EU, hvilket kan have en negativ effekt på det indre marked.

6.3.2. Relativ vurdering

Den konkurrerende opfattelse kendes under navnet "den relative tankegang". Den relative tankegang lægger vægt på en dataansvarliges egen konkrete forhold og dennes egen viden, samt viden den dataansvarlige kan indsamle fra andre.[50]

Det skal her tages med i vurderingen, om den dataansvarlige har de reelle midler og muligheder for at kunne identificere enkeltpersoner. Fokusset ligger dermed ikke kun på, om der er nogen, der kan identificere vedkommende. Fokusset ligger på, om der er en realistisk og rimelig mulighed for, at den dataansvarlige kan identificere enkeltpersoner på baggrund af de oplysninger, de har i deres varetægt eller har adgang til.[51]

Rimelighedsbetragtningen, som anvendes ved denne vurderingsform, udspringer fra databeskyttelsesforordningens betragtning 26, 2 og 3 pkt. Som lyder således:

"*For at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende. For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling." [52]*

[50] Ibid. s. 214
[51] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679, betragtning 26, 3. pkt.
[52] Ibid.

Fokus i denne opfattelse ligger dermed på rimelighedsbegrebet og derfor ikke elementet om "en anden person". Derudover skal der i denne opfattelse også medtages de objektive forhold, som nævnt i betragtningen.

Den relative vurdering kan, på baggrund af det ovenstående, anses for at være en mildere vurdering af, hvornår oplysninger skal anses for at være personoplysninger. Det har den betydning, at hvis man lægger vægt på denne vurderingsmetode, så vil der være flere situationer, hvor man kan undgå at ende indenfor personoplysningsbegrebet og dermed databeskyttelsesforordningen, så man ikke vil være omfattet af de samme restriktioner. Det kan gøre det lettere for selskaber o.lign at lave databehandling i EU og dermed mindske omkostninger og procedure for denne slags behandling. Det kan dog svække beskyttelsen for borgerne i EU.

6.3.3. Opsummering

Den store forskel på de to vurderinger er dermed, hvad der bliver lagt vægt på. Absolut vurdering, som beskrevet i ovenstående afsnit om absolut vurdering, fokuserer på begrebet "en anden person" og bliver derigennem en meget omgribende fortolkning af begrebet. Hvorimod vægtningen i den relative vurdering ligger på rimelighedsbegrebet og fortolkningen af dette. Det har den betydning, at der vil være flere situationer, hvor denne fortolkning kan betyde, at reglerne i databeskyttelsesforordningen ikke længere finder anvendelse for behandlingen. Det er endnu ikke konkluderet, hvilken tankegang der anses for korrekt, hvilket specialet senere vil komme ind på, hvori det også forsøger at besvare spørgsmålet om, hvilken af disse vurderinger de forskellige tilsynsmyndigheder lægger vægt på, samt hvilken vurdering EU-domstolen anvender i konkrete situationer.

6.4 Pseudonymisering

Forståelsen af begrebet pseudonymisering er vigtigt for at kunne differentiere mellem pseudonymiserede personoplysninger og anonymiserede oplysninger, hvilket også vil have en betydning for dette speciale og dets analyse.

Pseudonymisering er en legaldefinition, der findes i databeskyttelsesforordningens art. 4. stk. 1 nr. 5. Pseudonymisering er en metode, hvorpå den dataansvarlige eller databehandleren forsøger at skjule identiteten på den registrerede, der behandles personoplysninger om. En personoplysning er pseudonymiseret, når det kræver supplerende oplysninger for, at kunne re-identificere den registrerede. Oplysningen kan kun betegnes som pseudonymiseret, hvis de supplerende oplysninger, der er krævet for at identificere den registrerede, opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger. [53]

Pseudonymiserede personoplysninger er stadig dækket af databeskyttelsesforordningen, grundet pseudonymiserede personoplysninger stadig anses for at være en personoplysning i henhold til reglerne i databeskyttelsesforordningen. Dette skyldes, at pseudonymiseringen af oplysninger ikke fjerner muligheden for at kunne identificere en registreret, men derimod bare beskytter og besværliggøre processen for at kunne identificere den, som oplysningerne omhandler.[54]

Pseudonymisering spiller en rolle for flere af artiklerne, der findes i databeskyttelsesforordningen, herunder art. 32, der omhandler behandlingssikkerhed. Det er en af de oplistede relevante metoder til at beskytte den registrerede, og denne bliver ofte anvendt, da det er en effektiv og forholdsvis let metode til at implementere det første lag af beskyttelse af personoplysningerne.[55]

Det er vigtigt at forstå, at pseudonymisering og anonymisering er to forskellige begreber og ikke har den samme betydning for den dataansvarlige og databehandlerens ansvar under forordningen. Hvor pseudonymisering er en måde, hvorpå man kan beskytte personoplysninger, fjerner anonymisering (i teorien) muligheden for at kun identificere den

[53] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679
[54] Databeskyttelsesforordningen og databeskyttelsesloven (Nielsen, & Lotterup, 2025, s. 271)
[55] EDPB's "guidelines 01/2025 on pseudonymisation" s. 10-11

registrerede helt. Det er dermed vigtigt at have for øje, hvilken af metoderne, man har udført. Hvad der kræves for, at beskyttelsen kan kaldes anonymisering, bliver beskrevet i nedenstående afsnit.

6.5. Anonymisering

Anonymisering betyder at omdanne registreredes personoplysninger til anonyme oplysninger i databeskyttelsesforordningens forstand. Det vil sige, at det ikke skal være muligt for personer at identificere, hvem oplysningerne omhandler. Hvis oplysningerne reelt er anonyme, finder databeskyttelsesforordningen ikke anvendelse på disse oplysninger, og man skal dermed ikke overholde de regler eller opfylde kravene, der findes i databeskyttelsesforordningen.[56]

Anonymisering anvendes netop med det formål at falde uden for databeskyttelsesforordningens materielle anvendelsesområde, som er fundet i art. 2 stk. 1., og som lyder således:

"*Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.*"

Hvis art. 2 stk. 1. i databeskyttelsesforordningen ikke omfatter den behandling, der foretages af visse oplysninger, så falder behandlingen udenfor databeskyttelsesforordningens anvendelsesområde. Dette er suppleret af legaldefinitionen af personoplysninger i art. 4 nr. 1. samt betragtning 26 af databeskyttelsesforordningen, hvori EU–kommissionen beskriver, at databeskyttelsesprincipperne ikke bør finde anvendelse på, hvad der kaldes anonyme oplysninger.[57]

Anonyme oplysninger har en meget streng fortolkning inden for det databeskyttelsesretlige område. Hvad mange i dagligdagen vil kalde for anonymiserede personoplysninger, ville oftere være, hvad databeskyttelsesforordningen kalder pseudonymiserede personoplysninger. Dette skyldes identifikationskravet fra databeskyttelsesforordningens art. 4 nr. 1. "*enhver*

[56] Databeskyttelsesforordningen og databeskyttelsesloven (Nielsen, & Lotterup, 2025, s. 260)
[57] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679

form for information om en identificeret eller identificerbar fysisk person", sammenholdt med databeskyttelsesforordningens betragtning 26, som gør det gældende at for, at vurdere om, der er tale om identificerbare personer, så skal alle rimelige midler, som kan anvendes af dataansvarlig eller en anden person, tages med i vurderingen.[58]

Disse to krav skaber en meget høj barriere for at kunne kalde en oplysning anonym, og gør dermed reel anonymisering efter forordningen en krævende og streng proces.

Pseudonymiserings- og anonymiseringsbegreberne og forståelsen af disse, samt vurderingen af hvornår der er tale om hvilken, har en stor betydning inden for databeskyttelse, og for om man skal overholde kravene inden for databeskyttelsesforordningen eller ej. Begge begreber vil ses inddraget i den senere analyse, herunder i forbindelse med hvordan domstolen vurderer disse begreber og deres anvendelsesområde. Derudover vil begreberne også anvendt i forbindelse med undersøgelsen af, hvordan tilsynsmyndighederne vurderer personoplysningsbegrebet.

6.6. Tilsynsmyndigheder

Som nævnt tidligere i specialet, er det pålagt medlemslandene at have en eller flere uafhængige tilsynsmyndigheder, der skal sikre og kontrollere overholdelse af databeskyttelsesforordningen.[59] En af måderne hvorpå dette sikres, er ved tilsynsmyndighedernes afgørelser. Tilsynsmyndighedernes afgørelser kan derudover også anvendes til at udlede praksis på området, hvilket både kan vise de registrerede, hvilke rettigheder disse har, herunder også hvor langt disse strækker, samt vise virksomheder og organisationer, hvilke regler de skal overholde og hvordan.

Eftersom tilsynsmyndighedernes afgørelser kan anvendes til at udlede praksis på området, er det vigtigt at tilsynsmyndighederne på tværs af landegrænser vurderer og fortolker ens, da dette ellers vil skabe mere forvirring på området. Af den grund vil der i et senere afsnit blive analyseret nogle afgørelser afsagt af forskellige tilsynsmyndigheder, for at undersøge, hvorvidt disse vurderer personoplysninger ud fra den absolutte eller relative vurdering.

[58] Ibid.
[59] Ibid. art. 51

7. EU-domstolens afgørelser

I det følgende afsnit vil der blive analyseret fire forskellige EU-domme, som omhandler identifikationskravet til personoplysninger, samt hvordan EU-domstolen vurderer om dette er opfyldt. Dommene analyseres i kronologisk rækkefølge for at se på, hvordan vurderingen af personoplysninger har udviklet sig, samt for at vise, hvordan den tidligere retspraksis har en stor betydning for, hvordan EU-domstolen vurderer i efterfølgende sager. Dommene der bliver lagt fokus på i dette afsnit vil være C-582/14, C-434/16, C-604/22 og C-413/23. Henholdsvis også kaldet Breyer-dommen, Nowak-dommen, IAB Europe-dommen og SRB-dommen.

7.1. C-582/14 Breyer

Faktum fra Generaladvokatens vurdering

Denne dom er fremsat i 2016, før databeskyttelsesforordningen, og dermed afsagt med udgangspunkt i Databeskyttelsesdirektivet 95/46. Begrebet personoplysninger er i det tidligere gældende direktiv dog næsten identisk med legaldefinitionen i databeskyttelsesforordningen, hvorfor dommens præmisser stadig ses anvendelige. Dette støttes også af EU-dommen C-597/19, der gør det klart at praksis fra før databeskyttelsesforordningen stadig kan anvendes, så længe der er kongruens mellem det skrevne i databeskyttelsesdirektiv 95/46 og Databeskyttelsesforordningen.[60]

Sagen omhandler internetprotokoladresser (herefter IP-adresser). IP-adresser identificerer en specifik anordning f.eks. en computer. IP-adressen bliver meddelt til en given server, som webstedet har, når man som bruger besøger dette websted. I denne sag er det Forbundsrepublikken Tyskland, der lagrer IP-adresser på brugere, der besøger deres databaser, selv efter tilslutningen er ophørt.[61]

[60] C-597/19, præmis 107.
[61] C-582/14, generaladvokatens forslag til afgørelse M. Campos, præmis 22-24.

Tvisten, som sagen omhandler, er *" I denne sag er det omtvistet, hvorvidt dynamiske ip-adresser er en personoplysning som omhandlet i artikel 2, litra a), i direktiv 95/46/EF . Spørgsmålet kræver først og fremmest en afgørelse af, hvilken betydning det har, at det ikke er indehaveren af webstedet, men derimod tredjemand (internetudbyderen i denne sag), der råder over de yderligere oplysninger, som er nødvendige for at identificere brugeren"* - Sag C-582/14, generaladvokatens forslag til afgørelse M. Campos, præmis 5.

Problemet ligger i, at Forbundsrepublikken Tyskland lagrer IP-adresser på de personer, der tilgår deres databaser, selv efter tilslutningen er ophørt. Sagen blev anlagt af Breyer, som tabte i første instans, men han fik medhold i appellen, hvilket betyder, at forbundsrepublikken Tyskland ikke bør lagre IP-adresser efter at søgning er ophørt.[62] Kravet om ophør blev begrundet i, at brugeren afslører personoplysninger, når man tilgår systemet, og denne registrering må ikke gemmes, medmindre det er nødvendigt for at kunne genetablere adgang til telekommunikationstjenesten, hvilket er tilladt efter tysk lov.[63]

Der vil i dette afsnit blive gået i dybden med parternes anbringender, idet parterne tydeligt går ind og anvender de to forskellige vurderingsmetoder, som dette speciale omhandler. Det ses dermed essentielt at have begge siders argumentationer med i specialet. Disse anbringende har ikke nogen reel retskildeværdi, men de giver en god forståelse af, hvordan de to forskellige vurderinger kan bruges i praksis og som argumentation for vurderingen af personoplysningsbegrebet.

Parternes anbringender fra generaladvokatens dokument:

Generaladvokaten kommer i sin vurdering ind og forklarer de to parters argumentation for, hvorfor og hvorfor der ikke er tale om personoplysninger i den konkrete sag. Dette er med til at skabe baggrunden for den endelige vurdering af, hvilken af de to vurderinger der skal anvendes. Indledningsvis frembringer generaladvokat M. Campos, Patrick Breyers argumentation for, hvorfor der i denne konkrete sag er tale om personoplysninger efter databeskyttelsesdirektiv 95/46.

" Ifølge Patrick Breyer er personoplysninger også oplysninger, som kun teoretisk set kan kombineres, dvs. på baggrund af en abstrakt potentiel fare. Det er uvæsentligt, om denne

[62] Ibid, præmis 24-25.
[63] Ibid, præmis 27.

kombination sker i praksis. Efter Patrick Breyers opfattelse betyder den omstændighed, at et organ kan have relativt vanskeligt ved at identificere en person på grundlag af ip-adressen, ikke, at denne person ikke er i fare […]" - Sag C-582/14, generaladvokatens forslag til afgørelse M. Campos, præmis 32.

Breyer går her ind og argumenterer for, at oplysninger altid skal anses for personoplysninger, hvis de relaterer sig til en person, samt hvis der er en teoretisk mulighed for, at man kan identificere personen, uanset hvor teoretisk og besværlig denne mulighed måtte anses for at være. Breyer bruger her den absolutte vurdering, som gennemgået i afsnit 6.3.1 i dette speciale, af personoplysninger, som sit argument for, hvorfor registreringen og lagringen af hans IP-adresse er et brud på databeskyttelsesdirektivet.

" […]For at afgøre, om de angiver oplysninger om en »identificerbar« person i henhold til samme bestemmelse, bør identificerbarheden undersøges på baggrund af et »subjektivt« kriterium. Dette følger efter den tyske regerings opfattelse af 26. betragtning til direktiv 95/46, i henhold til hvilken der kun skal tages højde for de hjælpemidler, der »med rimelighed« kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person. En sådan præcisering tyder på, at EU-lovgiver ikke har ønsket at lade situationer, hvor det er objektivt muligt for tredjemand at foretage identificering, omfatte af anvendelsesområdet for direktiv 95/46." Sag C-582/14, generaladvokatens forslag til afgørelse M. Campos, præmis 33.

Det kan ses ud fra det ovenstående citat, at Forbundsrepublikken Tyskland derimod gør det gældende, at de dynamiske IP-adresser ikke skal anses for at være personoplysninger, da de ikke anser det for muligt at kunne identificere personen, disse IP-adresser omhandler ud fra rimelige hjælpemidler. De mener derfor, at fokus skal ligge på en relativ vurdering af personoplysningsbegrebet, idet vurdering skal foretages ud fra den reelle mulighed for at kunne identificere en person på baggrund af de oplysninger, som objektivt kan ses rimelige at anvende.

Forbundsrepublikken Tyskland går her ind og argumenterer for, at en vurdering af, hvorvidt en oplysning er en personoplysning efter direktivet, skal ske efter anvendelse af den relative vurdering af kravet om identifikation. Det er dermed ikke nok, at der eksisterer en mulighed for identifikation, men det skal også være en objektiv realistisk mulighed.
Forbundsrepublikken Tyskland argumenterer videre for denne holdning i præmis 34, hvor de

gør det klart, at de mener, man skal fortolke reglerne i henhold til formålet med direktiv 95/46. I samme præmis udtaler de også:

"Behovet for at beskytte fysiske personer kan betragtes på en anden måde afhængig af, hvem der er i besiddelse af oplysningerne, og hvorvidt de råder over de nødvendige hjælpemidler til at anvende dem til at identificere disse personer." - Sag C-582/14, generaladvokatens forslag til afgørelse M. Campos, præmis 34.

Hertil argumenterer Forbundsrepublikken Tyskland for, at de ikke selv har de oplysninger, der skal til for at identificere personerne, oplysningerne omhandler, idet disse kun er tilgængelige for internetudbyderne, og internetudbyderne ikke har hjemmel til at videregive disse oplysninger, samt at Forbundsrepublikken Tyskland dermed heller ikke har hjemmel til at modtage disse oplysninger.

Det kan på denne baggrund ses, at de to sider argumenterer ud fra hver deres vurderingsmetode, herunder de to metoder, som dette speciale omhandler, nemlig den absolutte vurdering, som Breyer argumenterer for, og den relative vurdering som Forbundsrepublikken Tyskland argumenterer for.

Efter parternes argumentation nu er gennemgået, vil analysen gå ind og se på, hvordan EU-domstolen vurderer og bruger de argumentationer, som de to parter har gjort gældende for hver af deres argumenter.

Vedr. det første præjudicielle spørgsmål:

Det første spørgsmål, som EU-domstolen anmodes om at besvare, lyder således:

"Med det første spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 2, litra a), i direktiv 95/46 skal fortolkes således, at en dynamisk ip-adresse, som en udbyder af online-medietjenester registrerer i forbindelse med en søgning foretaget af en person på en internetside, som denne udbyder gør tilgængelig for offentligheden, i forhold til den nævnte udbyder udgør en personoplysning som omhandlet i denne bestemmelse, når kun en tredjemand, i det foreliggende tilfælde denne persons internetudbyder, råder over den yderligere viden, der kræves for at kunne identificere denne person." - C-582/14, præmis 36.

Domstolen henviser i første omgang til, at der allerede foreligger en dom, Scarlet Extended C-70/10, der har taget stilling til, om IP-adresser skal anses for at være en personoplysning.

Det blev i den konkrete sag vurderet, at IP-adresser er en personoplysning, men dette er set ud fra internetudbydernes perspektiv, eftersom de har direkte adgang til hjælpemidlerne til at kunne identificere.[64] Domstolen lægger også vægt på, at spørgsmålet her vedrører dynamiske IP-adresser, og ikke statistiske IP-adresser, hvilket generaladvokat M. Campos tillige gør i sit forslag til afgørelse.[65] Dynamiske IP-adresser ændrer sig over tid modsat statiske, som forbliver de samme. Domstolen udtaler herom:

"I denne henseende skal det først bemærkes, at det er ubestridt, at en dynamisk ip-adresse ikke udgør en oplysning, der vedrører en »identificeret fysisk person«, for så vidt som en sådan adresse ikke direkte afslører identiteten på den fysiske person, der ejer den computer, fra hvilken søgningen på en internetside finder sted, og heller ikke identiteten på en anden person, der kunne anvende denne computer." - C-582/14, præmis 38.

Den første konklusion fra Domstolen er derfor, at dynamiske IP-adresser i sig selv ikke vurderes at være en personoplysning.

Domstolen fortsætter dog i præmis 39 med at fokusere på, at det skal vurderes om en sådan dynamisk IP-adresse kan udgøre en personoplysning grundet en tredjepart, på baggrund af de hjælpemidler, som parten kan have, der kan gøre det muligt at identificere en person. Det kan hermed ses, at vægtningen af vurderingen ligger på, om eksistensen af hjælpemidler hos tredjepart er nok til at konkludere, at der er tale om personoplysninger.

Domstolen lægger vægt på betragtning 26 fra direktiv 95/46, som beskriver, hvornår der er tale om personoplysninger, idet der heri bliver beskrevet, ligesom betragtning 26 af databeskyttelsesforordningen, at "*alle hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse, af den registeransvarlige og af »enhver anden person«* (…) C-582/14, præmis 43.

Domstolen lægger ved præmis 44-48 vægt på, at det skal vurderes, hvad der skal forstås ved begrebet "rimeligt" for Forbundsrepublikken Tyskland, og deres mulighed for at kunne identificere en person gennem de dynamiske IP-adresser. Det bliver udtrykkeligt gjort klart, i præmis 46, at dette ikke kan være gældende, hvis der er tale om en ulovlig adgang til oplysningerne. Her støtter domstolen sig op af generaladvokatens forslag til afgørelse præmis

[64] C-582/14, præmis 33.
[65] C-582/14, generaladvokatens forslag til afgørelse M. Campos, præmis 49.

68. Det kan dermed konkluderes, at der skal være tale om en lovlig adgang til hjælpemidlerne, for at hjælpemidlerne kan kvalificeres som rimelige.

"Selv om den forelæggende ret har præciseret i sin forelæggelsesafgørelse, at den tyske lovgivning ikke tillader internetudbyderen direkte at overføre den yderligere viden, der er nødvendig for identificeringen af den registrerede, til udbyderen af online-medietjenester, synes der imidlertid under forbehold af de efterprøvelser, der i denne henseende skal foretages af den forelæggende ret, at findes lovlige veje, der gør det muligt for udbyderen af online-medietjenester, bl.a. i tilfælde af angreb på netværk, at henvende sig til den kompetente myndighed, for at denne kan tage de nødvendige skridt for at opnå disse oplysninger hos internetudbyderen og for at foranledige strafferetlig forfølgning ." - C-582/14, præmis 47

Det kan ses i dette citat, at domstolen går ind og laver en konkret vurdering af rimeligheden og lovligheden af Folkerepublikken Tysklands mulighed for at få adgang til de hjælpemidler, der skal til for at kunne identificere vedkommende. Domstolen lægger sig her dermed op ad den relative vurdering af begrebet personoplysninger. Fokus ligger her ikke på, om der er en anden, der har de supplerende oplysninger, der skal til for at kunne identificere personen, men derimod, om det er muligt for Forbundsrepublikken Tyskland at modtage de hjælpemidler og ekstra oplysninger, der skal til for at identificere personen.

Eftersom der findes en lovlig vej for Folkerepublikken Tyskland til at modtage de supplerende oplysninger fra udbyderen af online-medietjenester, og at der er en procedure for, at dette kan ske, så skal dynamiske IP-adresser anses for at være en personoplysning. Det vigtige ligger dog i, at domstolen går ind og laver denne adskillelse af om oplysningerne bare eksisterer, eller om det reelt er muligt for Folkerepublikken Tyskland at modtage disse supplerende oplysninger.

Domstolen konkluderer på baggrund heraf:

"[…] *at en dynamisk internetprotokoladresse, som en udbyder af online-medietjenester registrerer i forbindelse med en søgning foretaget af en person på en internetside, som denne udbyder gør tilgængelig for offentligheden, i forhold til den nævnte udbyder udgør en personoplysning som omhandlet i denne bestemmelse, når udbyderen råder over lovlige hjælpemidler,"* - C-582/14, præmis 65, punkt 1.

Domstolen siger derfor, at eftersom udbyderen råder over lovlige hjælpemidler til at foretage identifikation, så er disse IP-adresser personoplysninger. Domstolen slår dermed fast, at et vigtigt krav i forbindelse med vurderingen af rimelige hjælpemidler efter betragtning 26 er, at disse skal være lovlige.

7.1.1. Delkonklusion

Sagen giver et stærkt indblik i, hvad EU-domstolen lægger vægt på, når de vurderer personoplysningsbegrebet samt kravet om identifikation, og dette danner et fundament for, hvordan personoplysningsbegrebet skal forstås i forhold til spørgsmålet om "anden person", og hvad der anses for "rimelige midler". Det konkluderes, at for at de supplerende oplysninger kan anses for at være "rimelige hjælpemidler", så skal der være tale om lovlige hjælpemidler.

EU-domstolen anvender i denne sag den relative vurdering, hvilket ses idet, de går ind og laver en konkret vurdering af, hvorvidt der er tale om rimelige hjælpemidler i forbindelse med identifikationen af de registrerede. Det ses dermed også, at EU-domstolen ikke anvender den absolutte vurdering i denne konkrete sag, da IP-adresserne havde været personoplysninger allerede, idet en tredjepart ligger inde med supplerende oplysninger, der vil kunne anvendes til identifikation, hvis de havde anvendt denne vurdering.

Sagen er, som tidligere nævnt, fra før databeskyttelsesforordningen, men det kan ses i andre EU-domme, at EU-domstolen stadig lægger vægt på Breyer-sagen og dens argumenter, når de afgører lignende sager hvor spørgsmålet om, hvad der skal anses for at være en personoplysning, bliver et fokuspunkt.[66] Det ses også i senere afsnit af dette speciale, at flere tilsynsmyndigheder også henviser til denne dom, når disse går ind og vurderer personoplysningsbegrebet.

[66] Se f.eks. C-413/23 P.

7.2. C-434/16 – Nowak

Faktum

Peter Nowak var en regnskabselev, der havde været igennem nogle regnskabsprøver, hvor han dumpede en af de eksamener, han var oppe til. Nowak klagede over, at han dumpede eksamen for fjerde gang, men blev afvist af klagekomiteen. Dette fik Peter Nowak til at indgive en anmodning om indsigt i sine personoplysninger, hvilket han har ret til jf. direktiv 95/46, da/hvis dette omhandler hans egne personoplysninger (retten til indsigt). Det blev afvist med begrundelsen, at der ikke var tale om personoplysninger.[67]

Nowak henvendte sig til den tilsynsførende for databeskyttelse for at anfægte denne begrundelse. Hvor den tilsynsførende svarede tilbage I juni 2010 med en mail der bl.a. sagde ” *»prøvebesvarelser i almindelighed ikke bliver behandlet [med henblik på databeskyttelse] […] da dette materiale i almindelighed ikke vil udgøre personoplysninger«*.” – C-434/16, præmis 21.

Nowak klagede over denne afgørelse.

Klagen blev lagt på is henfør den relevante databeskyttelseslovgivning, hvori man ikke behøver at behandle useriøse klager eller usaglige klager.

Sagen endte med at komme hele vejen til den øverste instans i Irland (Supreme Court), som var usikker på, om en eksamensafgørelse er en personoplysning. De foreligger dermed to spørgsmål til EU Domstolen, som lyder:

”»1) Kan oplysninger, der er nedskrevet/givet som svar af en deltager i forbindelse med en faglig prøve, være personoplysninger som omhandlet i direktiv 95/46/EF?

2) Hvis svaret på det første spørgsmål er, at alle eller nogle af sådanne oplysninger kan være personoplysninger som omhandlet i direktivet, hvilke faktorer er da relevante for at afgøre, om en sådan besvarelse i givet tilfælde er personoplysninger, og hvilken vægt bør sådanne faktorer tillægges?« ”– C-434/16, Præmis 26.

Fokus for dette speciale er på identifikationskravet, og hvordan EU-domstolen fokuserer på dette, så kun deres vurdering af dette vil blive taget med i denne analyse.

[67] C-434/16, præmis 18-20.

Om de præjudicielle spørgsmål

Indledningsvis lægger Domstolen fokus på, om der er tale om en identificerbar person efter direktiv 95/46's artikel 2, litra a).

"Ifølge denne bestemmelse forstås »ved identificerbar person […] en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet«." – C-434/16, Præmis 28.

Det ovenstående viser artiklen, som den fremstod i direktivet, og som domstolen foretog deres vurdering ud fra.

Domstolen gør det gældende i præmis 29-30, at der ikke kan være tvivl om, at en deltager i en faglig prøve er en fysisk person, udover dette anfægter de den tilsynsførendes argument om, at eksaminator ikke kan identificere personen, eksamensrettelsen omhandler.

" *i direktiv 95/46, er det ikke påkrævet, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person[…], Det er i øvrigt ubestridt, at i det tilfælde, hvor eksaminator ikke kender deltagerens identitet ved rettelsen af den pågældendes besvarelse i forbindelse med en prøve, råder den enhed, som afholder prøven, derimod over de nødvendige oplysninger til uden vanskeligheder eller tvivl at identificere deltageren ved hjælp af den pågældendes identifikationsnummer, som er anbragt på prøvebesvarelsen eller på dennes omslag, og således til at tillægge denne besvarelsen.*" – C-434/16, Præmis 31.

Domstolen tager her stilling til spørgsmålet om identifikation, og hvem der har mulighederne for at foretage denne identifikation. Domstolen vurderer utvetydigt, at det ikke har betydning om, eksaminatoren kan identificere personen ud fra de oplysninger, de sidder inde med, på den baggrund at brancheorganisationen, som har ansvaret for disse oplysninger, uden problemer kan identificere personen. Udover dette gør de det klart, at det ikke har betydning om alle oplysninger er ved en enkelt person, men at det derimod bare skal være muligt for den, der sidder inde med informationen, at fremskaffe de nødvendige hjælpemidler til at identificere den registrerede.

Det er vigtigt her at bemærke, at domstolen her ikke vurderer, at bare fordi det anses for muligt at identificere personen, så er der tale om personoplysninger. De går derimod ind og ser på, hvem der egentlig har ansvaret for oplysningerne, heri brancheorganisationen, da det er dem, der står for afholdelsen af prøven og ikke eksaminatoren. Vurderingen skal derfor

foretages ud fra hvilke informationer, brancheorganisationen har adgang til, og dermed de muligheder, de har for identifikation, hvorfor det ikke kan bestrides, at de har muligheden for at identificere Nowak. Konklusionen bliver dermed at identifikationskravet i definitionen af personoplysninger er opfyldt.

Resten af sagen går ind og diskuterer, om en eksamensbesvarelse kan anses for at være personoplysninger. Konklusionen bliver at det kan den godt, fordi de kommentarer der er til en eksamensrettelse anses for at være en personoplysning, idet det handler *om* Nowak.[68] Det bliver dermed konkluderet, at evalueringen af opgaven samt svarene er en personoplysning, men ikke selve eksamensspørgsmålene, dog er argumentationen for denne del ikke vigtig for specialets undersøgelsesområde, hvorfor dette ikke vil blive gennemgået yderligere.

7.2.1. Delkonklusion

Denne dom viser, at når der skal vurderes om en person er identificerbar, så skal der ses på de rimelige midler, som dataansvarlige som helhed ligger inde med, og ikke bare den enkelte person, som behandler oplysningerne, hvilket i denne sag er eksaminator. Idet eksaminatoren arbejder for en større organisation, som anses for dataansvarlige, så er det ikke den enkelte person, men her brancheorganisationen, der i sidste ende afholder eksamen.

[68] Ibid. præmis 62.

7.3. C-604/22 IAB Europe

Faktum

IAB Europe er en sammenslutning, der står for at forbinde selskaber, der vil købe reklamepladser på hjemmesider, hjemmeside-ejerne og persondatamæglere. Sammenslutningen er til for at sikre sig, at denne kæde af udbydere overholder databeskyttelsesforordningen, men samtidigt at det gøres på den letteste og mest effektive måde. De har skabt et framework ved navn TCF "transparency & consent framework", for at opnå det fremsatte formål, som lige nævnt, når de handler med reklamepladsen og personoplysninger på markedet, gennem en auktionslignende platform kaldet "open-RTB".[69]

For at kunne sikre sig, at denne behandling følger reglerne for databeskyttelsesforordningen, og dermed sikrer sig, at det er de rigtige hjemler, der bliver anvendt, så skal den besøgende på webstedet afgive sit samtykke, for at dennes personoplysninger bliver behandlet til reklameformål. Til dette bruges en såkaldt CMP (Consent Management Platform), som de besøgende på hjemmesiderne (herefter registrerede) afkrydser deres tilladelser i. CMP'en giver også den besøgende mulighed for at modsætte sig behandlingen af deres personoplysninger, som behandles på baggrund af andre hjemler som f.eks. legitim interesse.[70]

Tilladelserne, de registrerede giver på hjemmesiderne, bliver herefter gemt i en såkaldt TC-string (Transparency and Consent String*)*, hvilket er en lagring af disse præferencer, som dermed let og hurtigt kan deles med persondatamæglerne og reklameplatforme, for at kunne lave deres transaktioner efter de præferencer, som den registrerede har angivet og/eller modsat sig. Der placeres udover dette en cookie på de registrerede egne apparater, for at apparatet også husker, at den ikke skal stille dette spørgsmål igen. Kombineres disse to systemer, så kan de forbindes med en registreredes IP-adresse og derigennem identificere personen, som oplysningerne omhandler.[71]

[69] C-604/22 IAB Europe, præmis 21-23.
[70] Ibid, Præmis 24.
[71] Ibid, Præmis 25.

Disse systemer er der af flere lande, herunder Belgien, blevet klaget over i forhold til om de overholder databeskyttelsesforordningen, som antaget. Den belgiske tilsynsmyndighed har været inde og undersøge disse klager, og har derefter oprettet en sag imod IAB Europe, hvori de hævder, at IAB Europe er dataansvarlig for disse oplysninger. Det skyldes, at den belgiske tilsynsmyndighed mener, at IAB Europe har mulighed for at identificere de registrerede, hvis oplysninger bliver behandlet. IAB Europe anfægter, at der er tale om personoplysninger fra deres side af, da de ikke mener, at de med rimelighed kan anses for at have mulighed for at identificere de registrerede, da de ikke har adgang til alle de nødvendige hjælpemidler.[72]

Sagen nåede hele vejen til appeldomstolen i Belgien, som fremsatte to spørgsmål til EU-domstolen med ønske om afklaring. Der vil i dette projekt kun bliver fokuseret på spørgsmål 1, som lyder således:

" a)Skal [databeskyttelsesforordningens] artikel 4, nr. 1[)], [...], sammenholdt med [chartrets] artikel 7 og 8 [...], fortolkes således, at en tegnrække, som på en struktureret og maskinlæsbar måde fanger en internetbrugers præferencer i forbindelse med behandlingen af dennes personoplysninger, udgør en personoplysning som omhandlet i førnævnte bestemmelse i forhold til (1) en brancheorganisation, der stiller en standard til rådighed for sine medlemmer, hvormed den oplyser disse om, hvorledes den førnævnte tegnrække skal genereres, lagres og/eller distribueres, og (2) de parter, der har implementeret denne standard på deres websites eller i deres [applikationer], og på denne måde får adgang til denne tegnrække?

b)Har det herved nogen betydning, at implementeringen af standarden medfører, at denne tegnrække er til rådighed sammen med en IP-adresse?

c) Skal [det første spørgsmåls delspørgsmål] a) + b) besvares anderledes, såfremt denne regelgivende brancheorganisation ikke selv har nogen lovmæssig adgang til de personoplysninger, som inden for denne standard behandles af dens medlemmer?"
- C-604/22, præmis 31.

[72] Ibid, Præmis 27-29.

EU-Domstolens vurdering af det første præjudicielle spørgsmål

Til besvarelsen af ovenstående spørgsmål slår domstolen fast i sin vurdering, at man skal ind og analysere præcist, hvad ordlyden er af artikel 4 nr. 1 i databeskyttelsesforordningen, samt hvad formålet med denne artikel er. De fokuserer på ordene "enhver form for information", samt at der ved "identificerbar fysisk person" skal forstås enhver direkte eller indirekte identificerbar fysisk person.[73]

"*Derudover præciseres det i 26. betragtning, at for at afgøre, om en person er »identificerbar«, bør »alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende«. Denne ordlyd antyder, at for at en oplysning kan kvalificeres som »personoplysning« som omhandlet i denne forordnings artikel 4, nr. 1), er det ikke påkrævet, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person (jf. analogt dom af 19.10.2016, Breyer, C-582/14, EU:C:2016:779, præmis 43)*." - C-604/22, præmis 40.

Domstolen går her ind og slår fast, at Breyer-dommens fortolkning af, hvad der skal anses for at være en identificerbar person, stadig er den målestok, som bruges til at vurdere identifikationskriteriet. Domstolen går endvidere ind i en dybere fortolkning i de efterfølgende præmisser og pointerer, at det ikke er nok at kigge på informationen selv, for at vurdere om den er nok til at identificere en person, men derimod også på, om der findes supplerende materiale, der kan lægges sammen med den specifikke information for at kunne identificere en person. Det er en analog anvendelse af, hvad domstolen kommer frem til i Breyer-dommen, som bliver nævnt ovenfor. De går også ind og fastsætter, ligesom i Breyer-dommen, at det ikke er et krav, at de krævede oplysninger, for at kunne identificere en person, skal findes ved en dataansvarlig, men skal derimod anses som, om der er flere der tilsammen kan identificere den registrerede. [74]

"For det andet er det ligeledes ubestridt, at når de oplysninger, der er indeholdt i en TC String, er forbundet med en identifikator, såsom bl.a. IP-adressen på en sådan brugers

[73] Ibid, præmis 35.
[74] Ibid, Præmis 40.

udstyr, kan de gøre det muligt at skabe en profil på den nævnte bruger og effektivt identificere den person, der specifikt er berørt af sådanne oplysninger." - C-604/22, præmis 44.

Domstolen går her ind og kigger på den konkrete mulighed for, om en TC string kan anses for at bruges til at identificere en registreret og vurderer uden tvivl, at hvis man forbinder TC-strengen med en identifikator, som IP-adresser i denne sag, så gør det de registrerede identificerbare. Her viser domstolen, at identificerbar-begrebet ikke bare fokuserer på en specifik oplysning, men hvad en samling af flere oplysninger tilsammen kan udlede. Domstolen fokuserer her på at vurdere, hvilke metoder der skal til for at kunne identificere en person.

"Det fremgår i øvrigt af de sagsakter, som Domstolen råder over, og navnlig af afgørelsen af 2. februar 2022, at IAB Europes medlemmer er forpligtet til efter anmodning at meddele IAB Europe alle de oplysninger, der gør det muligt for selskabet at identificere de brugere, hvis oplysninger fremgår af en TC String. [...]

[...] fremgår det således, at IAB Europe i overensstemmelse med det i 26. betragtning til databeskyttelsesforordningen anførte råder over rimelige midler til at identificere en bestemt fysisk person ud fra en TC String ved hjælp af de oplysninger, som IAB Europes medlemmer og andre organisationer, der deltager i TCF, er forpligtede til at meddele IAB Europe." - C-604/22, præmis 48-49.

Her kan det ses, at domstolen lægger vægt på begrebet "rimelige midler" fra databeskyttelsesforordningen betragtning 26. De følger dermed i dette eksempel direkte den relative vurdering, samt fastholder retspraksis fra Breyer-dommen. Fokus ligger ikke kun på, om der er en anden, der har oplysninger i deres varetægt til at identificere personen, men også om det kan anses for at være rimeligt at forvente, at IAB Europe kan få adgang til de supplerende oplysninger, som de skal bruge for at kunne identificere personen oplysningerne omhandler. I denne situation har IAB Europe de rimelige midler på den baggrund, at de kan kræve de ekstra oplysninger, som skal til for identifikationen, udleveret.

Konklusionen på dommens første spørgsmål bliver dermed, at en TC-string skal anses for at være en personoplysning i databeskyttelsesforordningens forstand, da alle fire krav er opfyldt

fra artikel 4. nr 1, derunder at IAB Europe har muligheden for at kunne identificere personerne, som TC-strengen stammer fra. Dette skyldes ikke, at de selv sidder inde med de krævede oplysninger, men at de har rimelige midler til at kunne skaffe disse supplerende oplysninger og herefter identificere de registrerede.

7.3.1. Delkonklusion

Denne sag illustrerer godt, hvor domstolen lægger vægtningen, når de skal vurdere identifikationskravet. De tager begge parametre med fra databeskyttelsesforordningens betragtning 26, herunder "en anden person" samt "rimelige midler". Det kan dog ses i deres vurdering, at de lægger stor vægt på, at det ikke er nok, at der er en anden, der har oplysninger, men at det også bliver vurderet, om midlerne, der anvendes, kan anses for at være rimelige. Det er dermed ikke nok, at det skal anses for muligt, at en eller anden i verdenen kan identificere personerne, men at IAB Europe har en *rimelig* mulighed for at få udleveret disse oplysninger fra personen/enheden, der sidder inde med de supplerende oplysninger.

7.4. C-413/23 SRB

Faktum

Den fælles afviklingsinstans SRB skulle stå for at lave en afviklingsordning af banken Banco Popular Espanol (herefter kaldet BPE). I forbindelse med denne afvikling blev revisionsselskabet Deloitte valgt til at vurdere værdiansættelsen i forskellen mellem den valgte form for afvikling og en almindelig insolvensbehandling. Målet med dette var at se, om BPE's aktionærer og kreditorer ville have fået mere ud af en almindelig insolvensbehandling.[75]
Aktionærerne samt kreditorerne fik derefter chancen for at blive hørt i sagen, om hvorvidt de mente, at en anden afviklingsform kunne have øget kompensation. De fik dermed muligheden for at kritisere den valgte afviklingsform. Denne høringsperiode kørte over en længere periode, hvor de berørte kunne udøve retten til at blive hørt. Deloitte fik ansvaret for at gennemgå realiteten i de bemærkninger, som de berørte havde sendt ind.[76]

Der var ud over dette ansatte i afviklingsinstansen, der havde til opgave at behandle de bemærkninger, der var blevet modtaget af de berørte. Der var tale om et begrænset antal ansatte, samt at disse ansatte ikke havde adgang til de personoplysninger, der tilhørte de berørte. Oplysningerne var erstattet af en alfanumerisk kode i forsøg på at pseudonymisere disse personoplysninger. De bemærkninger, der blev vurderet identiske, blev derefter samlet til enkelte vurderinger, for at mindske antallet af bemærkninger.[77]

De relevante bemærkninger, som havde været igennem to filtreringsprocesser hos SRB, blev derefter overført til Deloitte i pseudonymiseret form. Det blev til 1104 bemærkninger, der blev fremsendt til Deloitte. Det var dermed kun SRB, der sad inde med de oplysninger, der skulle til for at kunne identificere personerne, som oplysningerne relaterede sig til.[78]

De berørte i sagen sendte derefter samlet en klage ind til EDPS med den begrundelse, at SRB havde tilsidesat oplysningspligten, idet de ikke var blevet informeret om, at disse

[75] C-413/23, præmis 10-13.
[76] Ibid, præmis 14-21.
[77] Ibid, præmis 22-25.
[78] Ibid, præmis 23-28.

bemærkninger ville blive videresendt til en tredjemand, her Deloitte. EDPS endte med at konkludere, at det er korrekt, at oplysningspligten i artikel 15 i forordning 2018/1725 var blevet tilsidesat.[79]

Efter SRB bad EDPS om at revurdere på baggrund af nye oplysninger, kom EDPS frem til, at der var tale om pseudonymiserede personoplysninger med den begrundelse, at der var tale om personoplysninger, og de havde sendt Deloitte en alfanumerisk kode, der gjorde det muligt for Deloitte at knytte besvarelserne til de enkelte berørte. Oplysningerne skal dermed behandles efter reglerne for personoplysninger. EDPS vurderer, at sanktioner ikke er nødvendige for denne overtrædelse grundet de tekniske og organisatoriske foranstaltninger, men SRB skulle i fremtiden sikre sig, at de berørte, i lignende sager om evt. overførsel af deres personoplysninger, blev informeret.[80]

SRB appellerede denne beslutning med påstand om annullering, samt at EDPS's afgørelse, erklæres ulovlig. Retten afviste anden påstand om erklæring af ulovlighed, men tog den første påstand om realitetsbehandling og annullerede den omtvistede afgørelse.[81]

Sagen har fokus på forordning 2018/1725, som omhandler beskyttelsen af fysiske personer, når deres oplysninger bliver behandlet af unionens institutioner o.lign. Det er dermed ikke direkte databeskyttelsesforordningen, som denne sag vurderes ud fra, men dennes beskrivelse, krav og anvendelse af begreberne "personoplysninger" og "identifikations" er ens med databeskyttelsesforordningens. Afgørelsen kan dermed godt bruges til at se, hvordan domstolen behandler dette område

Første anbringende for EU Domstolen.
Første anbringende lyder således:

"Med det første anbringende har EDPS i det væsentlige gjort gældende, at Retten begik en retlig fejl ved fortolkningen af artikel 3, nr. 1) og 6), i forordning 2018/1725 ved at fastslå, at appellanten i den omtvistede afgørelse med urette havde konkluderet, at de i det foreliggende tilfælde omhandlede oplysninger udgjorde personoplysninger. Det første anbringende består

[79] Ibid, præmis 29-30.
[80] Ibid, Præmis 31-34.
[81] Ibid, præmis 37-38.

af to led. Det første led vedrører den i denne forordnings artikel 3, nr. 1), fastsatte betingelse, hvorefter oplysningen er »om« den fysiske person, og det andet led vedrører den i samme bestemmelse fastsatte betingelse om, at denne person er »identificerbar«." - C-413/23, præmis 43.

Dette anbringende er opdelt i to led. Det ene led er om oplysningerne er "om" en person, hvor det andet led fokuserer på identifikationskravet. Fokus vil ligge på andet led, da dette er mest relevant for specialets problemformulering.[82]

Parternes argumenter andet led, første klagepunkt:
EDPS lægger fokus på kravet om "en anden person" i deres argumentation for, hvorfor der her er tale om en personoplysning, og på baggrund af dette skal det anses muligt at identificere den person, oplysningen omhandler.

"de dataansvarlige eller »en anden person« skal kunne identificere den registrerede med den omhandlede information. Når det ikke er angivet, hvem der skal kunne foretage denne identifikation, er det tilstrækkeligt, at den registrerede kan identificeres." - C-413/23, præmis 65.

Det kan ses her, at EDPS lægger stor vægt på kravet om "en anden person" og lægger sig dermed fra start tæt op ad den absolutte vurderingsmetode. De bruger dette argument over for domstolen for at appellere for, at SRB behandlede personoplysninger og videresendte disse personoplysninger til Deloitte. De gør det derudover også gældende, at lovgiver under udførelsen af denne lov med vilje har gjort begrebet og kravene brede for at indramme så mange behandlinger som muligt under denne lov.[83] Argumentationen her er dermed, at domstolen bør anse det som muligt, at nogen kan identificere personerne bag oplysningerne, og da formålet med loven er at ramme bredt, så bør dette være nok til, at SRB og deres behandling er omfattet af denne.

[82] Ibid.
[83] Ibid. præmis 66

EU-domstolen vurdering af andet led, første klagepunkt

EDPS gør det til dette klagepunkt gældende, at hvis det ikke er specificeret, hvem der skal kunne identificere en person efter forordningen 2018/1725, så må det anses for tilstrækkeligt at *en eller anden* kan identificere vedkommende.[84] Der må på baggrund af dette synspunkt være tale om personoplysninger for alle parter vedrørende denne sag.

EU-domstolen går ind og støtter EDPS's argumentation for, at disse pseudonymiserede oplysninger, som er sendt til Deloitte, som udgangspunkt kan anses for personoplysninger, da loven ikke specificere, hvilket synspunkt man skal se på det fra.[85]

"Det skal i denne henseende bemærkes, at det følger af artikel 3, nr. 1), i forordning 2018/1725, at en information skal vedrøre en »identificeret eller identificerbar« fysisk person for at kunne kvalificeres som en personoplysning i denne bestemmelses forstand. Anvendelsen af denne forordning forudsætter således principielt en undersøgelse af, om den registrerede er identificeret eller identificerbar ved den omhandlede information." - C-413/23, præmis 69-70.

EU-domstolen slår dermed fast, ligesom de tidligere domme, at der skal være tale om identificerbare personer for, at der kan være tale om personoplysninger. De siger derefter også, at det dermed er en nødvendighed at gå ind og undersøge, om det anses for muligt at identificere personerne oplysningerne vedrører ud fra den information, man har til rådighed. Diskussionen bliver dermed, om de gældende oplysninger, som Deloitte sidder ind med, er nok til at identificere personerne. EDPS lavede den fejl, at konkludere, at der er tale om personoplysninger uden at gå ind i den specifikke sag og realitetsbehandle muligheden for identifikation.

"[...]
»pseudonymisering« forudsætter, at der findes oplysninger, der gør det muligt at identificere den registrerede. Selve eksistensen af sådanne oplysninger er til hinder for, at de

[84] Ibis, præmis 63
[85] Ibid, præmis 68

oplysninger, der har været genstand for pseudonymisering, i alle tilfælde kan anses for at være anonyme oplysninger, der er udelukket fra anvendelsesområdet for denne forordning.

I tredje række forholder det sig ikke desto mindre således, at det krav om separat opbevaring af identificerende oplysninger samt tekniske og organisatoriske foranstaltninger »for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person«, der er foreskrevet i nævnte forordnings artikel 3, nr. 6), indikerer, at pseudonymiseringen bl.a. har til formål at undgå, at den registrerede kan identificeres alene med de pseudonymiserede oplysninger.

For så vidt som sådanne tekniske og organisatoriske foranstaltninger faktisk indføres, og de kan forebygge, at de pågældende oplysninger henføres til den registrerede, således at denne ikke eller ikke længere kan identificeres, kan pseudonymiseringen nemlig have indvirkning på den personlige karakter af disse oplysninger [...]" - C-413/23, præmis 73-75.

Domstolen går her ind og vurderer, hvad selve meningen med pseudonymisering er, og hvilken reel betydning det har for muligheden for at identificere de enkelte personer, som oplysningerne handler om. Det domstolen hermed diskuterer er, hvor meget betydning pseudonymisering kan have for identifikationskravet. De åbner dermed lidt op for muligheden for at pseudonymisering, mindsker muligheden for at identificere enkelte fysiske personer, og dermed bevæger det sig hen imod at fjerne identifikationsmulighederne, i hvert fald for nogle parter, hvilket også er målet med at pseudonymisere. Dette er dog kun, hvis de oplysninger, der pseudonymiseres og nøglen til at afpseudonymisere oplysningerne igen, holdes væk fra hinanden på en sikker og forsvarlig måde. Dette viser, hvordan domstolene lægger fokus på en realitetsvurdering af muligheden for at identificere de enkelte personer, og dermed ikke kun fokuserer på, at det ud fra oplysningerne er muligt for en eller anden person at identificere de registrerede.

Dette følger videre nede i præmis 77, hvor domstolen åbner op for muligheden, at oplysninger kan være anonyme ud fra Deloittes synspunkt, hvis ikke de har muligheden for at identificere de personer, der indgår i de fremsendte oplysninger fra SRB. De konkluderer dermed, at SRB, som dataansvarlig, ikke kan anfægte, at der er tale om personoplysninger, men ved videresendelsen til Deloitte, kan der være mulighed for, at der ikke længere er tale om personoplysninger, hvis vi vurderer fra Deloittes synspunkt.

"Domstolen har endvidere allerede fastslået, at et middel ikke med rimelighed kan tænkes bragt i anvendelse til at identificere den registrerede, når risikoen for en identificering i virkeligheden er ubetydelig, for så vidt som identificeringen af denne person er forbudt ved lov eller praktisk ugennemførlig, f.eks. på grund af det forhold, at den vil indebære en større indsats i tid, omkostninger og arbejde. [...]" - C-413/23, præmis 82

Det ses ud fra ovenstående, at EU-domstolen gør det klart, at det allerede er praksis, at oplysninger ikke automatisk er personoplysninger, bare fordi der eksisterer en mulighed for at identificere. Det vigtige i vægtningen er, om der findes en lovlig vej til at modtage de supplerende oplysninger, samt om denne metode overhovedet skal anses for mulig og relevant i den bestemte situation. Domstolen lægger dermed igen vægt på, at "rimelige midler" er den vigtigste faktor for, at der er tale om identificering, ikke bare om "en anden person" har de supplerende oplysninger. Dette følger godt i tråd med de domme, der også er blevet analyseret i dette speciale.

"Denne fortolkning drages ikke i tvivl af den af EDPS anførte omstændighed, hvorefter 16. betragtning, fjerde punktum, til forordning 2018/1725 tager sigte på den dataansvarlige eller »en anden person«. Det følger nemlig af ordlyden af dette punktum, som er anført i nærværende doms præmis 79, at der i dette punktum henvises til personer, som råder over eller kan tilgå midler, der med rimelighed kan tænkes at blive brugt til at identificere den registrerede." C-413/23, præmis 87.

Domstolen går her direkte ind og pointerer at kravet om en anden person, ikke er nok til at opfylde identifikationskravet, ligesom nævnt fra det tidligere citat så er EU-domstolens retspraksis og fremgangsmåde, at man skal se på, om der er en "anden person", der har de supplerende oplysninger, der skal til for identificere personerne. Derefter skal der ses på, om disse supplerende oplysninger kan indhentes med "rimelige midler". EDPS argumenterer for, at det er nok, at der er en anden person, der kan identificere, og det kan her ses, at de dermed argumenterer for den absolutte metode. Dette forkastes på den baggrund, at de i deres vurdering var nødt til at gå ind og undersøge om Deloitte i denne sag havde midlerne til at indsamle disse supplerende oplysninger. Domstolen slår dermed fast uden tvetydighed i denne dom, at det er den relative vurdering, der skal anvendes og ikke den absolutte

vurdering. EDPS' argument om at personoplysninger altid vil være personoplysninger bliver dermed forkastet af EU-domstolen, da dette vil kræve en konkret vurdering.

Første anbringende andet led andet klagepunkt

Dette klagepunkt handler om, hvorvidt retten som sagen er blevet appelleret fra har tilsidesat Breyer-dommen, idet denne retsinstans gik ind og konkluderede, at EDPS skulle have vurderet, om der var tale om personoplysningerne fra Deloittes synspunkt. EDPS gør det derimod gældende, som følge af Breyer, at selve eksistensen af lovlige hjælpemidler til at identificere de vedrørende personer er nok til at der er tale om personoplysninger. Samtidigt gør EDPS det gældende, at Deloitte ikke var dataansvarlig, men derimod havde en aftale med SRB og dermed ikke var nødsaget til at lave en fuldstændig vurdering af de rimelige midler.[86]

Afviklingsinstansen SRB har derimod gjort gældende, at EDPS bør have lavet en vurdering, om de registrerede var identificerbare på hver enkelte registrerede, og at dette skal ses ud fra modtagerens perspektiv og ikke afsenderens.[87]
Diskussionen går i dette klagepunkt ind og fokuserer på hvilket perspektiv man skal vurdere ud fra, når man ser på om den registrerede er "identificerbar", da dette ikke fremgår direkte af databeskyttelsesforordningen.
Domstolen konkluderer at det relevante perspektiv i denne sag, ud fra vi undersøger oplysningspligten, ville være afviklingsinstansen, da de skal informere den registrerede om mulig overførsel til tredjemand ved indsamlingstidspunktet, og det blev vurderet, at de havde alle muligheder for at identificere de registrerede.[88]

Sagen blev hjemsendt til retten, og der blev de to parter enige internt, og dermed blev sagen aldrig konkluderet af retten.[89]

[86] C-413/23, præmis 91-93.
[87] Ibid, præmis 96.
[88] Ibid, præmis 99-116, præmis 120.
[89] SRB pseudonymization case withdrawn from EU General Court (Iapp, 14.01.2026)

7.4.1. Delkonklusion

Sagen giver et stærkt indblik i hvilken vurdering EU-domstolen arbejder ud fra. De gør det klart i flere af deres præmisser, at EDPS' argumentation om, at personoplysninger skal anses for at være personoplysninger i alle tilfælde, ikke er korrekt. I vurderingen af rimelige midler er det vigtigt at have for øje de objektive faktorer, som f.eks. tid der skal bruges for at identificere, økonomien eller hvis loven gør det urimeligt at forvente, at den dataansvarlige eller andre parter, som Deloitte i denne sag, vil kunne identificere personerne, som oplysninger omhandler. Dommen giver dermed et stærkt indblik i, hvad der skal tages med i vurderingen, samt at personoplysninger ikke nødvendigvis er personoplysninger for alle, da det faktum at en institution kan identificere, ikke automatisk betyder, at en anden institution kan gøre det samme. Sagen er dermed endnu et tydeligt eksempel på, at domstolen lægger vægtning på "rimelige midler" og ikke bare "en anden person", og dermed at denne anvender den relative vurderingsmetode.

7.5. Sammenholdning af EU-dommene

Igennem dette afsnit har der været fokus på fire forskellige domme, der hver især går ind og kigger på muligheden for identifikation. Breyer-dommen startede diskussionen omkring hvilken vurdering, der skal anvendes ved fortolkningen af personoplysningsbegrebet, og her kom EU-domstolen frem til den konklusion, at da den dataansvarlige har interne procedurer, der gør det muligt *lovligt* at indhente de krævede supplerende oplysninger, så kan de godt identificere de registrerede, hvorfor der var tale om personoplysninger.

I Nowak-dommen går domstolen ind og slår fast, at der igen skal vurderes ud fra rimelige hjælpemidler. Fokus i denne sag ligger igen ikke på "en anden person", men de påpeger også, at det er vigtigt at kigge på rimelige midler ud fra den reelle dataansvarliges perspektiv, og ikke bare den enkelte, der behandler oplysningerne. Identifikationskravet skal dermed ikke bare fokusere på den enkelte, der arbejder med personoplysninger, men også den større helhed, som har adgang til personoplysningerne. Rækkefølgen på vurderingen skal dermed være: 1) Hvem er dataansvarlig i sagen? 2) Besidder den dataansvarlige de rimelige midler for at indhente supplerende oplysninger?

Efter Breyer og Nowak træder databeskyttelsesforordningen i kraft, og det bliver ud fra denne forordning at personoplysningsbegrebet og kravet for identifikation skal vurderes. Principperne og fremgangsmåden som hidtil anvendt er dog ført videre til denne forordning, som kan ses i de to domme, der stammer fra efter databeskyttelsesforordningen.

Selvom IAB-Europe sagen tager udgangspunkt i databeskyttelsesforordningen, kan det ses igennem dommen, at retspraksis og dets præmisser fra de to tidligere domme og fortolkningen, der følger heraf, ikke ændrer sig. Fokus i sagen bliver på, at det ikke er krævet, at en dataansvarlig skal sidde inde med alle de nødvendige oplysninger, men derimod bare skal kunne indhente de krævede supplerende oplysninger. Det bliver konkluderet, at IAB-Europe har alle de krævede midler for at indhente de supplerende oplysninger, der er nødvendige, og det bliver det udslagsgivende i denne sag, hvor domstolen vurdere, at der er tale om identificerbare personer, og dermed personoplysninger. Konklusionen fra domstolen giver et tydeligt billede af, at den tidligere retspraksis fra før databeskyttelsesforordningen, stadig er anvendelig efter ikrafttrædelsen af denne, og de samme præmisser gør sig gældende for vurderingerne, der følger forordningen.

Til sidst ses det i SRB-dommen, at domstolen fører retspraksis videre, som set i de tre andre domme. Domstolen vurderer tydeligt ud fra en relativ fortolkning, da denne går direkte ind og konkluderer, at "rimelige midler" skal anses ud fra de enkelte enheder, der sidder med personoplysningerne, til den givne behandling. I sagen blev det klart, at SRB ikke havde opfyldt deres oplysningspligt, og argumentationen fra SRB's side, om at det ikke skal anses for at være personoplysninger fra Deloittes synspunkt blev forkastet, idet man skal kigge på den enkelte behandling. Domstolen åbner op for muligheden, at der ikke er tale om personoplysninger fra Deloittes synspunkt, da de ikke har de "rimelige midler" til at kunne identificere personerne. Domstolen slår dermed fast, at fokus skal ligge på kravet om "rimelige midler", idet det kan udledes af deres argumentation, at hvad der er personoplysninger for nogle instanser, ikke nødvendigvis er personoplysninger for andre instanser.

Det er dermed utvetydigt igennem de fire domme, som går ind og behandler området vedr. identifikation og hvilken vurdering der er korrekt, den absolutte eller relative, at domstolen arbejder ud fra en relativ vurdering. Domstolen lægger i alle dommene vægt på kravet om "rimelige midler" og ikke på kravet om "en anden person". Kravet om "en anden person"

spiller kun en rolle, hvis det også er muligt for den mulige dataansvarlige ved hjælp af "rimelige midler" at indhente de supplerende oplysninger fra den "anden person".

Det kan dermed konkluderes på baggrund af disse domme, at EU-domstolen i de sidste mange år har anvendt den relative vurdering af begrebet personoplysninger, fra Breyer til i dag.

Det kan også være, at det er på denne baggrund, at EU-kommissionen, i form af Omnibus, har forsøgt at ændre definitionen på en personoplysning, samt kravet for hvornår der er tale om identificering. Dette vil blive gået mere i dybden med i afsnit 9.

8. Tilsynsmyndighed afgørelser

Det ses ud fra forrige afsnit, at EU-domstolen anvender den relative metode, når denne vurderer personoplysninger. Det ses derfor relevant at undersøge, hvorvidt tilsynsmyndighederne anvender samme fortolkning, eller om de går mod den standard, som der ud fra specialets tidligere analyse, er lagt af EU-domstolen.
Der vil i det følgende afsnit blive analyseret tre afgørelser fra forskellige tilsynsmyndigheder, for at undersøge, om disse tilsynsmyndigheder anvender samme vurdering af personoplysningsbegrebet. Der vil blive analyseret på afgørelserne 2023-211-0004, PS/00158/2022, SAN-2024-013, som er afsagt af henholdsvis den danske tilsynsmyndighed, den spanske tilsynsmyndighed og den franske tilsynsmyndighed.
Den første analyse omhandler en afgørelse afsagt af den danske tilsynsmyndighed, idet denne er juridisk mest relevant for os i Danmark. Herefter analyseres en afgørelse afsagt af den spanske tilsynsmyndighed og til sidst den franske tilsynsmyndighed, for at undersøge, hvorvidt disse fortolker og vurderer personoplysningsbegrebet ens.
Dette er ikke repræsentativt for, hvordan vurderingen foretages i hele EU, men dette kan bidrage til et indblik i, hvorvidt tilsynsmyndighederne generelt fortolker og vurderer ens, når det kommer til personoplysningsbegrebet.

8.1. Afgørelse fra den danske tilsynsmyndighed 2023-211-0004.

Faktum:

Denne afgørelse blev afsagt på baggrund af en henvendelse fra Alexandra Instituttet, som ønskede at dele et datasæt til udvikling af sprogteknologi, og de ønskede hertil den danske tilsynsmyndigheds (herefter datatilsynet) vurdering.[90] Datasættet behandler stemmeoptagelser af gerne op mod 2.000 personer af forskellige køn, alder og geografisk ophav. Datasættet vil blive renset, så direkte henførbare oplysninger som navn og adresse ikke er tilgængeligt, der vil dog stadig være visse oplysninger tilknyttet datasættet herunder alder, køn og omtrentlig

[90] Afgørelse 2023-211-0004, Resumé.

geografisk placering. Disse oplysninger er dog ikke med, hvis antallet af oplæsere i en gruppe er for få.[91]
Der bliver i afgørelsen taget stilling til to spørgsmål, herunder om der er tale om anonymisering, og om der er tale om særlige kategorier af personoplysninger. I denne analyse ses der bort fra spørgsmålet omkring særlige kategorier af personoplysninger, således at der kun analyseres ud fra den del af afgørelsen, der omhandler, hvorvidt datasættet er anonymiseret eller omhandler personoplysninger.

Datatilsynets vurdering:
I forbindelse med datatilsynets vurdering af, hvorvidt datasættet er anonymiseret, går datatilsynet ind og kigger på, hvad databeskyttelsesforordningen siger herom. Herunder fastlægger datatilsynet, at hvis der er tale om anonymisering, så finder databeskyttelsesforordningen ikke anvendelse på forholdet.[92]

"Omfattet af begrebet personoplysninger er ifølge bemærkningerne herefter oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer som f.eks. løbenummer. Omfattet vil ligeledes bl.a. være oplysninger, som foreligger i form af billede, personens stemme, fingeraftryk eller genetiske kendetegn.

Det er uden betydning, hvorvidt identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig, hvorfor også de tilfælde, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen." - 2023-211-0004, 3.1.1.

Her henviser Datatilsynet til Justitsministeriets betænkning nr. 1565/2017. Det ses heri, at en persons stemme kan være en personoplysning. Det er hertil ligegyldigt, hvorvidt det kun er "den indviede", der kan identificere personen ud fra dennes stemme.

I forbindelse med vurdering om, hvorvidt der er tale om personoplysninger henviser datatilsynet til de fire elementer i legaldefinitionen, og udtaler hertil: *"I nærværende tilfælde er spørgsmålet navnlig, om kravet om identificeret eller identificerbar er opfyldt."*[93]

[91] Ibid, 3.1.
[92] Ibid, 3.1.1.
[93] Ibid, 3.1.2.

Der lægges dermed kun vægt på elementet omkring identifikation i Datatilsynets vurdering.

Først undersøger Datatilsynet, hvorvidt en person kan anses for at være identificeret gennem dennes stemme. I denne forbindelse henvises der til artikel 29-gruppens udtalelse (som er gennemgået i afsnit 6.2.) idet Datatilsynet lægger vægt på "*... spørgsmålet om, hvorvidt den person, som oplysningerne vedrører, er identificeret eller ej, afhænger af omstændighederne i det pågældende tilfælde."* - 2023-211-0004, 3.1.2.

Hvorvidt en stemme er en personoplysning, er altså ikke en vurdering, der skal laves ud fra kun objektive faktorer, da man også skal inkludere omstændighederne i det pågældende tilfælde i vurderingen.

Som konklusion hertil vurderer Datatilsynet:

"Genkendelse af stemmen må imidlertid også forudsætte et forudgående kendskab til stemmen og personen bag. Venner, familie og øvrige nære relationer vil således med en vis sandsynlighed kunne identificere, hvem stemmen tilhører alene ved at lytte til denne. For den uindviede vil identificeringen være sværere.

[...]

Datatilsynet kan imidlertid ikke på baggrund de foreliggende oplysninger med tilstrækkelig sikkerhed fastslå, i hvilket omfang det er muligt for en bredere kreds af personer at identificere en person ud fra de omhandlede lydoptagelser, og at stemmen allerede derfor udgør en unik identifikator, der fører til, at de pågældende lydoptagelser skal anses som personoplysninger om en identificeret person." - 2023-211-0004, 3.1.2.

Det konkluderes dermed, at det muligvis vil kræve forudgående kendskab til vedkommende for at kunne identificere denne ud fra stemmen, og at Datatilsynet ikke med sikkerhed kan sige, at vedkommende er "identificeret", da det ikke kan fastslås, hvorvidt det er muligt for en bredere kreds at identificere vedkommende. Dette stemmer dog dårligt overens med Datatilsynets tidligere citat: "*Det er uden betydning, hvorvidt identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig, hvorfor også de tilfælde, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen."* 2023-211-0004, 3.1.1.

De to citater er modsigende, da det ene citat udtrykker en holdning for, at det er uden betydning, hvorvidt det kun er indviede, der kan identificere vedkommende ud fra dennes stemme. Med det andet citat siger Datatilsynet, at der i dette konkrete tilfælde ikke er tale om, at vedkommende nødvendigvis er identificeret, da det ikke er sikkert, at andre end de indviede vil kunne identificere denne. Det er derfor ikke tydeligt, hvilken af disse holdninger, der menes at være korrekt.

I forhold til hvorvidt vedkommende er "identificerbar", henviser Datatilsynet til betragtning 26 i databeskyttelsesforordningen, herunder "*bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende."* - 2023-211-0004, 3.1.2.

> *"Det er ikke en forudsætning, at den yderligere viden, som kræves for at identificere den pågældende, er i den dataansvarliges besiddelse. Det skal vurderes, om der findes hjælpemidler, for den dataansvarlige, som med rimelighed kan tænkes bragt i anvendelse. EU-Domstolen har præciseret, at det ikke er tilfældet, hvis identificeringen af den registrerede er forbudt eller praktisk ugennemførlig, f.eks. på grund af det forhold, at identificering vil indebære en større indsats i tid, omkostninger og arbejde, således at risikoen for en identificering i virkeligheden synes ubetydelig"* - 2023-211-0004, 3.1.2.

I forbindelse med ovenstående citat henviser Datatilsynet til Breyer-dommen (denne analyseres i afsnit 7.1). Eftersom der i citatet lægges fokus på de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse, tyder dette på, at Datatilsynet i denne sag anvender en mere relativ vurdering i forhold til personoplysningsbegrebet.

Datatilsynet gør det gældende, at alle vil have adgang til datasættet, eftersom dette offentliggøres på nettet. Til vurderingen af "rimelige hjælpemidler" udtaler Datatilsynet:

> *"Den nuværende teknologi og den teknologiske udvikling synes i den konkrete sag at være af afgørende betydning for vurderingen af, hvorvidt datasættet udgør personoplysninger, da stemmegenkendelsesværktøjer de senere år er blevet mere almindelige og lettilgængelige. Det forudsætter dermed ikke adgang til særlige værktøjer at kunne gennemføre sådanne analyser. Derudover kan det bl.a. nævnes, at stemmeanalyse allerede bliver brugt til*

identificering f.eks.. i straffesager, hvor det anvendes til at identificere mulige gerningsmænd og andre personer ud fra deres stemme.

[...]

Derudover har den teknologiske udvikling, herunder udbredelsen af kunstig intelligens, muliggjort efterligning af en persons stemme bl.a. til ondsindede formål. Der kan derfor være en interesse i for en ondsindet aktør at identificere personen bag lydoptagelsen med henblik på at bruge stemmeoptagelsen til at gennemføre målrettede it-sikkerhedsangreb (phishing) eller svindel." - 2023-211-0004, 3.1.2.

Det ses altså, at Datatilsynet går ind og vurdere, at den teknologiske udvikling gør det relativt nemt for andre personer at identificere vedkommende ud fra dennes stemme, hvorfor Datatilsynet også mener, at der er rimelige hjælpemidler, der kan bringes i anvendelse, hvorfor datasættet indeholder personoplysninger. Eftersom Datatilsynet går ind og laver denne konkrete vurdering af, hvorvidt der findes rimelige hjælpemidler, tyder dette igen på, at Datatilsynet anvender en relativ vurdering i forhold til personoplysningsbegrebet.

8.1.1.Delkonklusion:

Ud fra ovenstående ses det, at Datatilsynet anvender en relativ vurdering, når de vurderer personoplysningsbegrebet. Dette ses, da der i omhandlende sag, lægges fokus på vurderingen af rimelige hjælpemidler, frem for hvorvidt der er *nogen*, der kan identificere vedkommende. Datatilsynet modsiger dog sig selv i forbindelse med, hvorvidt det er tilstrækkeligt, at indviede kan identificere vedkommende efter justitsministeriets betænkning, til at de ikke kan konkludere tilstrækkeligheden af dette grundet uvished om størrelse på personkredsen, der kan identificere stemmen. Det skal dog bemærkes, at der i denne sag er tale om et datasæt, som alle vil have adgang til, hvorfor vurderingen af rimelige hjælpemidler foretages ud fra en meget stor personkreds, hvorfor standarden naturligt ligger lavt, hvilket under andre omstændigheder vil kunne være en indikator for en mere absolut vurdering.

8.2. Afgørelse fra den spanske tilsynsmyndighed PS/00158/2022

Faktum:

Denne sag startede, da en klager indsendte en klage til den spanske tilsynsmyndighed, hvori denne oplyste om flere medier, der havde offentliggjort en videooptagelse af et offer for gruppevoldtægts vidneforklaring på deres hjemmesider. Lydfilen blev offentliggjort for at illustrere nyheden om retssagen.[94]
Lydfilen blev senere fjernet fra hjemmesiderne, men var stadig tilgængelige på mediernes twitterprofiler.[95]
Der blev på baggrund af dette startet en indledende undersøgelse og derefter en sanktionsprocedure, da det blev konstateret, at filen havde været offentliggjort ved nyhedskanalen *20 MINUTOS EDITORA, S.L.*[96]
Den anklagede mente ikke, at der var beviser for, at der på deres hjemmeside havde været offentliggjort en lydfil uden forvrængning. Derudover mente de heller ikke, at der var tale om personoplysninger.[97] Det første punkt vurderes dog ikke relevant for denne analyse, hvorfor dette ikke vil blive behandlet yderligere.
Argumentet om, hvorvidt lydfilen er en personoplysning, er derimod essentielt for analysen. *20 MINUTOS EDITORA, S.L.* mente ud fra artikel 29-gruppens udtalelse om personoplysninger (som er gennemgået i afsnit 6.2.), at lydfilen ikke var en personoplysning, da offentliggørelse af en stemme ikke altid er en personoplysning. Herunder mente de ikke, at oplysningens art eller konteksten gjorde det muligt at identificere kvinden.[98]

Den spanske tilsynsmyndigheds vurdering:
Til at besvare *20 MINUTOS EDITORA, S.L.'*s påstand om, at stemmen i lydfilen ikke var en personoplysning, var den spanske tilsynsmyndighed inde og vurdere, hvorvidt dette var tilfældet.

[94] PS/00158/2022, baggrund 1. punkt.
[95] Ibid, 2. punkt.
[96] Ibid, 3. & 4. punkt.
[97] Ibid, 6. Punkt.
[98] Ibid, 6. Punkt.

"For det første, og uden at det berører en mere detaljeret gennemgang heraf i retsgrundlag IV i denne afgørelse, skal det bemærkes, at enhver persons stemme er en personoplysning, som identificerer vedkommende eller gør vedkommende entydigt identificerbar, uanset hvor mange personer der måtte kunne genkende stemmen." - PS/00158/2022, Retsgrundlag III

I ovenstående ses det, at den spanske tilsynsmyndighed modsat 20 MINUTOS EDITORA, S.L mener, at en stemme altid er en personoplysning, og så er det underordnet, om der er nogen, der kan genkende personen på baggrund af stemmen. Dette ses ud fra "*at enhver persons stemme er en personoplysning […] uanset hvor mange personer der måtte kunne genkende stemmen"*- PS/00158/2022, Retsgrundlag III.

Ud fra dette citat vurderer den spanske tilsynsmyndighed personoplysninger ud fra en mere absolut vurdering, idet fokusset ikke lægger på, hvorvidt nogen med rimelige midler vil kunne identificere personen. Der tages slet ikke stilling til, hvorvidt vedkommende kan identificeres ud fra ens stemme, idet der står "*uanset hvor mange personer der måtte kunne genkende stemmen"* - PS/00158/2022. Ud fra dette vil stemmen være en personoplysning, og så er det uden betydning om, der er én person eller 100 personer, der kan identificere vedkommende.

Efterfølgende går den spanske tilsynsmyndighed ind og siger, at stemmen passer med "enhver oplysning" i forhold til udtalelsen 4/2007 fra Artikel 29-Gruppen.[99]

"I det foreliggende tilfælde identificerer offerets stemme vedkommende direkte i vedkommendes omgivelser (forstået i bred forstand, der omfatter det familiære og det sociale), da, som det fastslås i den nævnte udtalelse 4/2007, "kan en fysisk person betragtes som »identificeret«, når vedkommende inden for en gruppe af personer »adskiller sig« fra alle andre medlemmer af gruppen". Og der er tale om en klar behandling, hvis stemmen er blevet videreformidlet via det pågældende kommunikationsmedium, i henhold til artikel 4, stk. 2, i GDPR.

Og det er klart, at enhver persons stemme kan føre til, at vedkommende i det mindste genkendes af dem, der tilhører offerets nærmeste omgangskreds, eller som på anden måde

[99] Ibid, Retsgrundlag III.

kender vedkommende. Tænk f.eks. på familiemedlemmer, kolleger, studiekammerater, venner fra sociale aktiviteter osv." - PS/00158/2022, Retsgrundlag III.

Det ses ud fra dette, at den spanske tilsynsmyndighed igen lægger vægt på udtalelsen fra Artikel 29-gruppen, idet denne udtaler sig, om at man kan være identificeret, når vedkommende adskiller sig fra andre medlemmer af gruppen. Der bliver også fra den spanske tilsynsmyndigheds side lagt vægt på, at vedkommendes nærmeste omgangskreds vil kunne genkende vedkommende ud fra dennes stemme. Dette tyder endnu en gang på, at den spanske tilsynsmyndighed vurderer mere absolut, da fokus ligger på, at *nogen* kan identificere vedkommende ud fra oplysningen, og dermed ikke hvorvidt det i realiteten er muligt at identificere vedkommende.

"Det er rigtigt, at der i nogle tilfælde er nuancer, der kan gøre det vanskeligt at identificere en person ud fra vedkommendes stemme, navnlig når der er helbredsproblemer, der forårsager dysfoni, når personen bevidst og frivilligt ændrer sin naturlige måde at tale på (som f.eks. ved efterligninger), og når stemmen forvrænges ved hjælp af tekniske midler. Men ingen af disse tilfælde gør sig gældende i den foreliggende sag." PS/00158/2022, Retsgrundlag III.

Her går den spanske tilsynsmyndighed ind og siger, at der kan være situationer, hvor det er mere besværligt at identificere en person ud fra sin stemme, men at dette ikke er tilfældet i denne sag. Den spanske tilsynsmyndighed udtalte dog intet om, hvorvidt dette ville ændre på, om der stadig er tale om en personoplysning.

Herefter beskriver den spanske tilsynsmyndighed, hvordan offeret også indirekte kan identificeres i forbindelse med andre oplysninger, som er offentliggjort i forbindelse med sagen. Den spanske tilsynsmyndighed kommer herefter ind på betragtning 26 i databeskyttelsesforordningen. Dertil siger de:
"*I denne henseende fastslår EU-Domstolens dom af 19. oktober 2016 i sag C-582/14 i sagen mellem Patrick Breyer og Bundesrepublik Deutschland, at »41 EU-lovgiverens anvendelse af udtrykket »indirekte« viser, at det for at betegne en oplysning som en personoplysning ikke er nødvendigt, at denne oplysning i sig selv gør det muligt at identificere den registrerede.*

42 Desuden fastslår betragtning 26 i direktiv 95/46, at man for at afgøre, om en person er identificerbar, skal tage hensyn til alle de midler, som den dataansvarlige eller enhver anden person med rimelighed kan anvende til at identificere den pågældende person.
43 I det omfang, at den nævnte betragtning henviser til de midler, som med rimelighed kan anvendes af såvel den dataansvarlige som af »enhver anden person«, tyder ordlyden heraf på, at det for, at en oplysning kan betegnes som »personoplysning« i henhold til artikel 2, litra a), i nævnte direktiv, er det ikke nødvendigt, at alle oplysninger, der gør det muligt at identificere den registrerede, befinder sig i én enkelt persons besiddelse." (understregningen er vores [Den spanske tilsynsmyndigheds])." - PS/00158/2022, Retsgrundlag III

I det ovenstående argumenterer den spanske tilsynsmyndighed ud fra Breyer-dommen (som bliver analyseret i afsnit 7.1.). Breyer-dommen var, som specialet også kom ind på tidligere, den EU-dom, hvor der for første gang rigtig tages stilling til absolut vs. relativ vurdering i forhold til personoplysningsbegrebet, hvorfor det er oplagt, at den spanske tilsynsmyndighed henviser til denne dom i sin afgørelse.
Præmis 42 i Breyer-dommen, som der henvises til, lægger vægt på, at man ved vurderingen skal tage hensyn til de rimelige midler, den pågældende person vil kunne tage i brug for at identificere vedkommende. Dette lægger op til, at der anvendes en mere relativ vurdering, og eftersom den spanske tilsynsmyndighed henviser hertil, kunne dette også tyde på, at de til en vis grad vurderer relativt.
I den efterfølgende del af citatet lægges vægten mere på, hvem der kan identificere vedkommende. Herunder har den spanske tilsynsmyndighed lagt meget vægt på, at det ikke er nødvendigt, at alle oplysningerne befinder sig ved én enkelt person. Dette ses ved at de har understreget "*er det ikke nødvendigt, at alle oplysninger, der gør det muligt at identificere den registrerede, befinder sig i én enkelt persons besiddelse."* - PS/00158/2022, Retsgrundlag III. Dette tyder igen på, at der anvendes en mere absolut vurdering, eftersom fokus meget ligger på, hvorvidt der er *nogen*, der kan identificere offeret, og ikke så meget på hvorvidt det er realistisk muligt, herunder med fokus på de rimelige midler.

8.2.1. Delkonklusion:

Ud fra ovenstående analyse ses det, at den spanske tilsynsmyndighed primært anvender en absolut tilgang til vurderingen af personoplysninger, men at der også er elementer af en relativ vurdering. Der er igennem afgørelsen flere steder, hvor den absolutte tilgang kommer til udtryk, herunder da den spanske tilsynsmyndighed udtaler følgende: "[...] *uanset hvor mange personer der måtte kunne genkende stemmen."* - PS/00158/2022, Retsgrundlag III, samt: "[...]*Og det er klart, at enhver persons stemme kan føre til, at vedkommende i det mindste genkendes af dem, der tilhører offerets nærmeste omgangskreds, eller som på anden måde kender vedkommende."* - PS/00158/2022, Retsgrundlag III.
Ved begge citater ligger fokusset på, hvorvidt *nogen* kan identificere vedkommende og ikke, hvordan det realistisk set er muligt ud fra anvendelsen af rimelige midler, herunder hvordan/om det er muligt for den dataansvarlige.
Den relative tilgang kommer til udtryk, idet den spanske tilsynsmyndighed henviser til Breyer-dommen og herunder, at der skal tages hensyn til de rimelige midler, der kan tages i anvendelse til identificeringen af vedkommende.
Den relative tilgang finder derfor til en vis grad anvendelse ved den spanske tilsynsmyndigheds vurdering i denne afgørelse, men deres generelle vurdering i afgørelsen er mere absolut.
Det skal dog her bemærkes, at denne sag handler om offentliggørelse af en stemme, og hvorvidt dette er en personoplysning. Eftersom sagen omhandler offentliggørelse af en mulig personoplysning, er det oplagt, at kredsen som der vurderes ud fra udvides, da der herved er mange flere personer, som potentielt kan identificere vedkommende.

8.3. Afgørelse fra den franske tilsynsmyndighed SAN-2024-013

Faktum:

Denne afgørelse er afsagt af Commission Nationale de l'Informatique et des Libertés (CNIL), som er den franske tilsynsmyndighed. Sagen omhandler selskabet Cegemdim Santé, som udvikler og sælger administrationssoftware til læger og andet sundhedspersonale, herunder f.eks. CROSSWAY, som gør det muligt for læger at administrere kalender og patientjournaler.[100] Virksomheden tilbyder lægerne (mod rabat) at tilmelde sig et observatorium, hvor dataene ryger ind i virksomhedens datastrømme, hvor dataene kan anvendes til undersøgelser og statistikker.[101] CNIL startede en undersøgelse af databehandlingen i forbindelse med dette, hvor det blev konkluderet at virksomheden overtrådte databeskyttelsesforordningen art. 5, stk. 1, litra a.[102]

Systemet fungerer på den måde, at en patient tildeles et unikt identifikationsnummer for en specifik læge i CROSSWAY-systemet. Nummeret er ikke baseret på nogen identitetsoplysninger, men er tilknyttet vedkommende medicinske og administrative data.[103]

Cegemdim Santé mener, at de omhandlede data er anonymiseret, hvorfor de ikke mener, at databeskyttelsesforordningen finder anvendelse på dataene.[104]

Parternes argumenter:

I forbindelse med at skulle vurdere, hvorvidt dataene er anonymiseret eller stadig kvalificeres som personoplysninger, kommer både CNIL og Cegemdim Santé med nogle argumenter.

Først nævner CNIL legaldefinitionen på personoplysninger og på pseudonymisering, samt påpeger at der ikke er en legaldefinition på anonymisering. Ydermere går de ind og nævner betragtning 26 i databeskyttelsesforordningen, herunder dennes indhold.[105]

[100] SAN-2024-013, præmis 5.
[101] Ibid, præmis 6 og 7.
[102] Ibid, præmis 9 og 12.
[103] Ibid, præmis 61.
[104] Ibid, præmis 24
[105] Ibid, præmis 38-42.

Herefter går CNIL ind og belyser EU-domstolens tidligere retspraksis, og dennes betydning for området, herunder Breyer-sagen, OC-sagen og IAB Europe.[106] Ydermere går CNIL ind og lægger vægt på artikel 29-gruppens udtalelser omkring anonymisering, hvor de udtaler:

"*...at en proces navnlig kan betegnes som anonymisering, når den modstår følgende tre typer risici:*

- individualisering, hvilket svarer til muligheden for at isolere en del af eller alle de registreringer, der identificerer en person i datasættet;
- korrelation, hvilket består i evnen til at sammenkæde mindst to registreringer, der vedrører den samme registrerede eller en gruppe af registrerede;
- inferens, som er muligheden for med stor sandsynlighed at udlede værdien af et attribut ud fra værdierne af en række andre attributter.
48. Hvis dataene ikke modstår de tre ovennævnte risikotyper, vil de ikke nødvendigvis blive betegnet som pseudonymiserede. De kan betegnes som anonyme, hvis den dataansvarlige kan påvise, at reidentifikation ikke er mulig ved hjælp af rimelige midler, dvs. at risikoen for reidentifikation er ubetydelig." - SAN-2024-013, præmis 47-48.

Det ses her, at hvis dataene modstår risikoen for individualisering, korrelation og inferens, så kan de betragtes som anonyme, da det dermed kan bevises, at den dataansvarlige ikke kan re-identificere personerne ved brug af rimelige midler. Det ses her, at der bliver lagt vægt på de rimelige midler, og hvorvidt disse vil kunne blive anvendt af *en dataansvarlig* til at identificere vedkommende. Det faktum, at fokusset ligger på de rimelige midler tyder på, at den franske tilsynsmyndighed vurderer relativt, når denne går ind og vurderer personoplysningsbegrebet.

Cegemdim Santé argumenterer mod, at der er tale om personoplysninger, ud fra følgende:

"[...] selv i tilfælde af identifikation af en patientkode, der er knyttet til de kendte oplysninger om den eftersøgte person i CROSSWAY-strømmen, fører dette ikke nødvendigvis til reidentifikation. Virksomheden hævder nemlig, at der kun er en vis sandsynlighed for, at de oplysninger, der findes i databasen, er oplysninger om den eftersøgte person. Virksomheden mener, at en række usikkerhedsfaktorer forhindrer reidentifikation, f.eks. fordi en person kan

[106] Ibid, præmis 43-46.

dele de kendte karakteristika med andre personer, eller fordi det ikke er muligt at vide, om den eftersøgte person er til stede i databasen eller ej." - SAN-2024-013, præmis 54.

Ud fra dette ses det, at virksomheden argumenterer for, at dataene ikke nødvendigvis kan knyttes til en bestemt person, selv hvis man identificerer ud fra en patientkode, da der kan være en række usikkerhedsfaktorer. Virksomheden argumenterer derfor for, at vedkommende ikke nødvendigvis vil kunne identificeres, selv hvis "pseudonymiseringen" knækkes.

CNIL argumenterer imod dette på den baggrund, at den voksende database af oplysninger vil gøre sandsynligheden for re-identifikation af enkelte personer tæt på en. Udover dette gør de det også gældende, at udskiftning af identifikator-kode minder mere om en pseudonymisering end en anonymisering. Henblikket med dette udskift af identifikator i sagen er med det formål at kunne følge op på den bestemte kode (en bestemt patient) i fremtiden, og dermed skal muligheden for at lægge fremtidige datasæt sammen med de nuværende tages med i betragtningen. CNIL gør det dermed gældende, at Cegedim Santé's argumentation om, at der kun er en vis sandsynlighed for re-identifikation, ikke er et tilstrækkeligt stærkt argument for at kunne bevise, at der er tale om anonymisering.[107]

CNIL's vurdering:

CNIL konkluderer, at:

"- på den ene side svarer denne fremgangsmåde, der består i at erstatte direkte identificerende data med indirekte identificerende data, nemlig en unik identifikator for den pågældende patient hos den samme læge, fuldstændigt til definitionen af pseudonymisering og gør det muligt at foretage en langsgående opfølgning af patienten;

- for det andet, da det er muligt på denne måde at isolere en person i datasættet og med tiden øge mængden af data, der vedrører vedkommende, er patientdataene tilstrækkeligt omfattende til at gøre det muligt at ophæve pseudonymiseringen ved hjælp af rimelige midler." - SAN-2024-013, præmis 62.

107 Ibid, præmis 59-60.

I den første del af argumentet, gør CNIL det klart, at fremgangsmåden direkte passer på definitionen af pseudonymisering, hvorfor dataene dermed ikke kan være anonymiseret, da dataene ikke kan være både pseudonymiseret og anonymiseret for den samme dataansvarlig.

I den anden del af argumentet lægger CNIL vægt på, at det er muligt ved hjælp af rimelige midler med tiden at ophæve pseudonymiseringen og derved identificere patienten. CNIL vurderer altså, at der er tale om personoplysninger, og ud fra at fokus ligger på, hvorvidt der er tale om rimelige midler, ses det, at CNIL anvender en mere relativ vurdering i forhold til personoplysningsbegrebet. Det ses ud fra ovenstående, at CNIL lægger vægt på vurdering af rimelige midler, frem for at vurdere ud fra, hvorvidt det er muligt for *nogen* at identificere vedkommende.

For at støtte argumentet om, at det er muligt at ophæve pseudonymisering ved brug af rimelige midler, demonstrerede CNIL, at det ud fra nogle få datalinjer var muligt at rekonstruere en 12-årigs sygdomsforløb.[108] I denne forbindelse udtalte CNIL, at:

"Den bemærker, at det ikke har krævet meget tid eller mange ressourcer: rapportøren har foretaget en analyse på baggrund af de data, som virksomheden har fremsendt, ved udelukkende at anvende Excel-software og den nomenklatur, som virksomheden har fremsendt, for at knytte de alfanumeriske koder til oplysninger om patienten og de udførte medicinske ydelser. I denne sammenhæng har rapportøren ikke gjort brug af tredjepartsdatakilder, f.eks. data fra datamæglere (data brokers) eller geolokaliseringsdata."
- SAN-2024-013, præmis 76.

Eftersom CNIL kun anvendte Excel-software og den nomenklatur, som fremsendt, til at rekonstruere den 12-åriges sygdomsforløb, styrker dette CNIL's argument, om at pseudonymisering kan ophæves med rimelige midler, hvorfor der vil være tale om personoplysninger og pseudonymisering og ikke anonymisering.

CNIL konkluderede, at der var tale om et pseudonymiseret datasæt og ikke et anonymiseret datasæt.[109]

[108] Ibid. præmis 63.
[109] Ibid, præcis 87.

8.3.1. Delkonklusion:

Det ses i det ovenstående, at CNIL's fokus har lagt på, hvorvidt det er muligt med rimelige midler at identificere de registrerede. Dette ses for eksempel ved, at CNIL beviser, at de kan rekonstruere et sygdomsforløb kun ud fra Excel-software og den nomenklatur, virksomheden fremsendte. Idet CNIL argumenterer og vurderer sagen ud fra de rimelige midler, tyder dette på en mere relativ vurdering i forhold til personoplysningsbegrebet. CNIL argumenterer på intet tidspunkt ud fra en mere absolut vurdering, hvilket ses idet det aldrig er et fokuspunkt, hvorvidt *nogen* kan identificere vedkommende ud fra dataene, men kun hvorvidt den dataansvarlige med rimelige midler vil kunne identificere vedkommende.

8.4. Sammenholdning af afgørelserne

Ud fra de tre ovenstående analyser, ses det, at de udvalgte tilsynsmyndigheder ikke fortolker og vurderer personoplysningsbegrebet ens.

Den danske tilsynsmyndighed anvender en relativ vurdering af personoplysningsbegrebet, dog anvendes der i den specifikke sag en meget stor personkreds til at vurdere, hvorvidt den registrerede kan identificeres, idet datasættet offentliggøres. Da personkredsen der vurderes ud fra, er stor, betyder dette at grænsen for, hvornår vedkommende kan identificeres, sættes lavere.

Den spanske tilsynsmyndighed anvender primært en absolut vurdering, da deres fokus ved vurderingen ligger på, hvorvidt *nogen* vil kunne identificere vedkommende. Der er dog også elementer i afgørelsen, som tyder på en relativ vurdering, herunder idet der henvises til Breyer-dommen og rimelige midler herunder.

Den franske tilsynsmyndighed anvender tydeligt den relative vurdering, hvilket ses idet, der lægges fokus på vurdering af de rimelige midler, som *en dataansvarlig* kan anvende til at identificere den registrerede.

Det bemærkes her, at der er flere ligheder mellem afgørelsen fra den danske tilsynsmyndighed og den spanske tilsynsmyndighed, herunder at begge sager omhandler oplysninger om stemmer, der offentliggøres. Det interessante i dette er at, tilsynsmyndighederne vurderer så forskelligt på to sager, der ligner hinanden betydeligt.

Det ses altså, at der i Spanien primært anvendes en absolut vurdering dog med elementer af en relativ vurdering, hvorimod der i Danmark og Frankrig anvendes en relativ vurdering.

Det kan dermed konstateres, at tilsynsmyndighederne ikke fortolker og vurderer personoplysningsbegrebet ens, hvilket kan skabe problemer og frustration for virksomheder, såvel som registrerede, da det er, ikke er tydeligt ud fra tilsynsmyndighedernes praksis, hvornår en oplysning er en personoplysning, og dermed om denne skal nyde beskyttelse under databeskyttelsesforordningen.

9. Omnibus

Den 19. november 2025 kom Europa Kommission med et forslag til ændring af forordningerne (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 og direktiv 2002/58/EF, (EU) 2022/2555 og (EU) 2022/2557, hvilket kaldes Den Digitale Omnibus eller Omnibus.[110]
Formålet med Omnibus-forslaget er at forenkle regelsættene og dermed gøre EU mere konkurrencedygtige.[111]
Dette ændringsforslag ses yderst relevant for specialet, idet Omnibus indeholder et forslag til ændring af legaldefinitionen af personoplysninger. Forslaget lyder, at personoplysningsbegrebet skal ændres så:

> *"[...] blive præciseret ved at fastslå, at oplysninger ikke skal betragtes som personoplysninger for en given enhed, når denne ikke har midler, der med rimelighed kan forventes at blive anvendt til at identificere den fysiske person, som oplysningerne vedrører. Som følge heraf vil en sådan enhed i princippet ikke være omfattet af nævnte forordnings anvendelsesområde."* - Den Digitale Omnibus artikel 3.

Dette forslag går derfor direkte ind og berører specialets undersøgelsesområde, idet personoplysningsbegrebet vil blive specificeret i forhold til relativ eller absolut vurdering. Forslaget lyder ud fra ovenstående på, at en oplysning ikke vil være omfattet af databeskyttelsesforordningen, hvis det ikke er muligt for "en given enhed" at kunne identificere vedkommende, som oplysningen omhandler, ud fra rimelige midler. Hvis ændringen vedtages, som beskrevet ovenfor, vil den nuværende betragtning 26, altså blive flettet ind i selve legaldefinitionen, idet denne netop beskriver forholdet omkring rimelige midler i forhold til vurdering af, hvorvidt der er tale om personoplysninger.
Idet forslaget har fokus på, hvorvidt der er tale om rimelige midler i vurderingen af, om der er tale om personoplysninger, lægger forslaget derfor op til en mere relativ vurdering. Det vil derfor være muligt, at visse former for pseudonymiserede data ikke er omfattet af selve

[110] Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om ændring af forordning (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 og direktiv 2002/58/EF, (EU) 2022/2555 og (EU) 2022/2557 for så vidt angår forenkling af det digitale regelsæt og om ophævelse af forordning (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 og direktiv (EU) 2019/1024 (den digitale omnibus)
[111] Ibid, 1. Baggrund for forslaget.

personoplysningsbegrebet. Det er dog umuligt helt at se bort fra den absolutte vurdering, idet det ikke vides konkret, hvad der menes med "en given enhed".
Forslaget vil dog muligvis kunne få den betydning, at vurderingen af personoplysningsbegrebet bliver mere ensrettet, idet dette måske fjerner tvivlen om, hvorvidt vurderingen skal bero på rimelige midler eller "en anden person".
En præcisering af personoplysningsbegrebet som foreslået i Omnibus, bør derfor skabe en mere ensartet praksis, og gøre det nemmere for såvel virksomheder, som registrerede, at konkludere, hvorvidt der behandles personoplysninger.

I forbindelse med at Omnibus er blevet offentliggjort, er EDPB og EDPS kommet med en fælles udtalelse omkring forslaget.[112]
Generelt forholder EDPB og EDPS sig positivt til lovforslaget, idet de mener, at Omnibus vil kunne styrke EU's konkurrenceevne og bidrage til en mere ensartet behandling af personoplysninger.[113]
EDPB og EDPS udtaler dog, at de har visse bekymringer i forhold til at ændre legaldefinitionen af personoplysninger.[114]
For det første gør EDPB og EDPS det gældende, at den foreslåede ændring forsøger at implementere retspraksis i lovgivning ud fra EU-domstolens C-413/23 (SRB-dommen, som er gennemgået i afsnit 7.4.).[115]
Det illustrerer, at dommen har været skelsættende, samt at der nu er opstået yderligere forvirring på området i forbindelse med dommen.

EDPB og EDPS mener dog, at en ændring i definitionen som foreslået, vil direkte ændre det materielle anvendelsesområde i databeskyttelsesforordningen, hvilket ikke stemmer overens med hverken charteret eller TEUF, som databeskyttelsesforordningen bygger på.[116]
De mener derfor ikke, at ændringen bør vedtages som foreslået, idet anvendelsesområdet vil ændres på en måde, der ikke stemmer overens med baggrunden for og formålet med databeskyttelsesforordningen.

[112] EDPB-EDPS JOINT OPINION 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)
[113] Ibid, 2. General remarks.
[114] Ibid.
[115] Ibid, 3.1.12.
[116] Ibid, 3.1.14.

I forhold til at forslaget bygger på SRB-dommen udtaler EDPB og EDPS også, at databeskyttelsesforordningen, herunder også personoplysningsbegrebet, skal fortolkes ud fra al retspraksis fra EU-domstolen og ikke kun ud fra en enkelt sag, hvorunder kun et enkelt element medtages.[117]
De gør det altså her gældende, at lovforslaget ikke stemmer overens med al retspraksis, hvorfor det dermed ikke kan bidrage til at udlede gældende ret med. Dette ses specifikt, da EDPB og EDPS udtaler:

"*The Proposal ignores the specific characteristics of the case and will undermine – rather than improve – legal certainty*." - EDPB-EDPS joint opinion 2/2026, 3.1.15.

Det ses altså, at de mener, at forslaget vil skabe mere usikkerhed omkring personoplysningsbegrebet end klarhed, idet forslaget kun bygger på et enkelt element fra en enkelt EU-dom.

"*In addition, the EDPB and the EDPS highlight that the proposed changes do not accurately reflect and clearly go beyond the CJEU jurisprudence. This is the case, in particular, of the last sentence of the proposed new text which specifies that 'such information <u>does not become</u> personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates. In the EDPS v SRB judgment, the CJEU confirmed its previous jurisprudence, by recalling that otherwise impersonal data <u>may become</u> personal in nature when they are put at the disposal of a recipient (any recipient) with means reasonably likely to be used to identify a data subject. The CJEU confirmed that, in such cases, those data are personal data both for the recipient and, indirectly, for the entity making the data available to the latter.*" - EDPB-EDPS joint opinion 2/2026, 3.1.16.

Det ses ud fra ovenstående, at EDPB og EDPS også mener, at forslaget på trods af, at være bygget på baggrund af SRB-dommen, faktisk ikke korrekt reflekterer denne dom. Forskellen skyldes, at forslaget til ændringen er negativt afgrænset i stedet for positivt.

[117] Ibid, 3.1.15

EDPB og EDPS udtaler dertil, at en negativ afgrænsning frem for en positiv, vil kunne betyde endnu mere forvirring på området, samt at det vil kunne betyde, at de dataansvarlige muligvis vil søge smuthuller, så de undgår at skulle overholde databeskyttelsesforordningen.[118]
Det ses dermed at EDPB og EDPS mener, at forslaget i praksis vil betyde mindre beskyttelse af personoplysninger, både idet forslaget vil skabe forvirring, men også idet at de dataansvarlige muligvis vil forsøge at finde smuthuller, så behandlingerne slet ikke er omfattet af databeskyttelsesforordningen og dermed ikke underlagt dennes krav til beskyttelse.

Ydermere gør EDPB og EDPS det gældende, at forslaget ikke tager højde for elementet "udpege" fra betragtning 26, samt at forslaget vil have en negativ betydning for anden lovgivning.[119] Dette skyldes, at der er anden EU-lovgivning, der bygger på samme definition af personoplysninger, hvorfor en ændring i denne ene lovgivning, vil betyde, at der ikke længere er kongruens mellem disse, hvilket vil kunne skabe yderligere forvirring på området. EDPB og EDPS endte derfor med kraftigt at fraråde at vedtage lovforslaget i sin nuværende form.[120]

Udover EDPB og EDPS' udtalelse om Omnibus har Max Schrems gennem NOYB (Non Of Your Business) også udarbejdet en rapport omkring lovforslaget, hvor han herunder kommer ind på mulige konsekvenser ved at ændre legaldefinitionen på personoplysninger.[121]
NOYB, og herunder også grundlæggeren Max Schrems, kæmper for at tech-giganter og andre overholder databeskyttelsesforordningen.[122]

I NOYB's analyse af Omnibus gives der et overblik af, hvad formålet med ændringen ville være, samt hvilke konsekvenser dette vil have, både for virksomheder, registrerede og tilsynsmyndighederne.[123]

[118] Ibid, 3.1.17-18.
[119] Ibid, 3.1.17 og 20.
[120] Ibid, 3.1.21.
[121] NOYB, *Digital Omnibus - First Analysis of Select GDPR and ePrivacy Proposals by the Commission version 3.0*
[122] *Max Schrems* (JUC, u.d.)
[123] NOYB, *Digital Omnibus - First Analysis of Select GDPR and ePrivacy Proposals by the Commission version 3.0,* Article 4(1) – Definition of 'Personal Data'

Analysen viser, at forslaget vil introducere en mere subjektiv (relativ) tilgang til vurderingen af personoplysninger, idet denne vil ekskludere visse former for pseudonymiseret data fra definitionen.[124]

Derudover kommer analysen, ligesom EDPB og EDPS' udtalelse også ind på, at eventuelle ændringer til definitionen skal stemme overens med den generelle forståelse af personoplysninger, herunder forståelsen i Chartret. Der lægges også i analysen vægt på, at ændringen kun følger EU-dommen, SRB, men ikke stemmer overens med al anden retspraksis fra EU-domstolen. Det nævnes også, at der vil være flere negative konsekvenser som f.eks. forvirring omkring gældende ret, og dataansvarlige der forsøger at undgå at være omfattet af databeskyttelsesforordningen. Derudover nævner analysen også, at det vil kunne betyde længere behandlingstid i forbindelse med klager til tilsynsmyndigheder.[125]
Max Schrems og NOYB ender med, ligesom EDPB og EDPS, at konkludere, at forslaget til ændringen ikke bør vedtages.[126]

Det bemærkes hertil, at forslaget omkring ændringen af legaldefinitionen muligvis er blevet fjernet fra Den Digitale Omnibus. Dette kan ses gennem et læk af en nyere version af forslaget, hvori ændring af legaldefinitionen ikke er med.[127] Dette er dog ikke blevet bekræftet fra nogle relevante officielle kilder.

[124] Ibid, Article 4(1) – Definition of 'Personal Data', Overview.
[125] Ibid.
[126] Ibid, Article 4(1) – Definition of 'Personal Data', Overview.
[127] EU member states' leaked Digital Omnibus compromise proposal eliminates revised GDPR definition of 'personal data' (iapp, 23. februar 2026)

9.1. Sammenfatning

Omnibus indeholder et forslag til ændring af legaldefinitionen af personoplysninger i databeskyttelsesforordningen. Ændringen vil implementere en relativ tilgang til vurderingen af, hvorvidt en oplysning er en personoplysning, idet visse pseudonymiserede data ikke vil være omfattet af definitionen, og dermed ikke være omfattet af databeskyttelsesforordningen. EDPB og EDPS er kommet med en fælles udtalelse omkring Omnibus, som ligesom NOYB's analyse af forslaget, indeholder en gennemgang af mulige konsekvenser ved vedtagelsen af ændringen til legaldefinititionen. Både udtalelsen og analysen ender med at konkludere, at ændringen ikke bør vedtages. Dette konkluderes på baggrund af, at ændringen ikke stemmer overens med anden EU-lovgivning eller Chartret, samt at ændringen bygger på retspraksis fra en enkelt sag, og at ændringen ikke stemmer overens med anden retspraksis. Derudover menes det, at ændringen vil skabe forvirring, smuthuller, længere behandlingstid ved tilsynsmyndigheder og flere bøder.

10. Konklusion

Det er igennem specialet blevet undersøgt, hvorvidt personoplysningsbegrebet skal fortolkes relativt eller absolut. Ved en relativ vurdering bliver der lagt fokus på, hvorvidt den registrerede kan identificeres ud fra rimelige midler. En absolut vurdering af begrebet, ligger fokus på, hvorvidt der er *nogen*, der kan identificere den registrerede. En fortolkning af personoplysningsbegrebet skal foretages ud fra legaldefinitionen af personoplysninger i databeskyttelsesforordningens art 4, stk. 1., og ud fra betragtning 26 i databeskyttelsesforordningen. Udover disse to elementer skal en fortolkning også foretages ud fra retspraksis, da dette kan være med til at klarlægge gældende ret.
For at kunne konkludere hvilken vurdering, der skal anvendes, har specialet derfor analyseret fire EU-domme på området. De udvalgte EU-domme er Breyer-dommen, Nowak-dommen, IAB-Europe-dommen, samt SRB-dommen.
I Breyer-dommen ses det, at EU-domstolen lægger vægt på de rimelige hjælpemidler, som kan anvendes til identifikation, samt at én part ikke behøver at have alle informationer, hvis man har en lovlig adgang til de supplerende oplysninger. I Nowak-dommen bliver det konkluderet, at man skal kigge på rimelige midler ud fra den dataansvarlige som helhed. I den konkrete sag betyder det, at der skal kigges på organisationen og ikke den specifikke eksaminator. EU-domstolen kommer i IAB-Europe-dommen ind på både "en anden person" og "rimelige hjælpemidler", men konklusionen ender med at være, at det ikke er tilstrækkeligt, at en anden person kan identificere vedkommende, da der skal være en *rimelig* mulighed for identifikation. I SRB-dommen gør EU-domstolen det klart, at der skal vurderes rimelige midler, og at man i denne vurdering skal medtage de objektive faktorer. Domstolen gør det også klart, at bare fordi noget er personoplysninger for en part, behøver det ikke være personoplysninger for en anden part. Det ses ud fra disse analyser, at EU-domstolen fortolker personoplysningsbegrebet ud fra en relativ fortolkning.

Efter analysen af hvilken vurdering EU-domstolen anvender, vurderes det relevant at undersøge, hvorvidt tilsynsmyndighederne anvender samme vurderingsform. I den forbindelse er der blevet analyseret tre afgørelser fra forskellige tilsynsmyndigheder, herunder fra den danske, spanske og franske tilsynsmyndighed.
Det kan ud fra disse analyser konkluderes, at tilsynsmyndighederne ikke vurderer og fortolker personoplysningsbegrebet ens. Den spanske tilsynsmyndighed fortolker begrebet ud

fra en mere absolut vurdering, hvorimod både den danske tilsynsmyndighed og den franske tilsynsmyndighed fortolker ud fra en relativ vurdering. Dette ses, da den spanske tilsynsmyndighed fokuserer på, hvorvidt det er muligt for *nogen* at identificere den registrerede, hvorimod den danske og franske tilsynsmyndighed går ind og vurderer, hvorvidt det er muligt ud fra rimelige hjælpemidler at kunne identificere den/de registrerede. Det kan derfor konkluderes, at det ikke er alle tilsynsmyndigheder, der følger den standard, EU-domstolen har lagt i forhold til hvilken vurdering, der er den korrekte.

Ud fra ovenstående kan det konkluderes, at personoplysningsbegrebet skal fortolkes ud fra en relativ vurdering, og at fokus ved vurderingen derfor skal være på, hvorvidt man ved brug af rimelige hjælpemidler vil kunne identificere den eller de registrerede.

EU-kommissionen kom i november 2025 med et ændringsforslag til blandt andet databeskyttelsesforordningen kaldet Den Digitale Omnibus eller i daglig tale Omnibus. I dette ændringsforslag er der blandt andet et forslag om at ændre legaldefinitionen på personoplysninger, så dette lægger op til en relativ vurdering. Forslaget kommer på baggrund af SRB-dommen, og ud fra dette vil visse pseudonymiserede data ikke være omfattet af personoplysningsbegrebet. I forbindelse med ændringsforslaget er EDPB og EDPS kommet med en fælles udtalelse herom, og Max Schrems er gennem NOYB kommet med en analyse heraf. Både udtalelsen og analysen kommer frem til visse negative konsekvenser, herunder blandt andet, at forslaget ikke stemmer overens med anden EU-lovgivning eller anden EU-retspraksis, hvilket vil kunne betyde, at der vil komme endnu mere forvirring på området. Derudover vurderes det, at flere dataansvarlige vil udnytte formuleringen til, at undgå at skulle overholde databeskyttelsesforordningen. Konklusionen på både udtalelsen og analysen bliver derfor, at forslaget ikke bør vedtages.

11. Diskussion

Som ses ud fra opgaven, bevæger tilsynsmyndighederne sig hen mod en relativ vurdering, når begrebet personoplysninger skal vurderes og fortolkes. Det kan ses, at den franske og den danske tilsynsmyndighed hovedsageligt støtter sig op af den relative vurdering, modsat Spaniens tilsynsmyndighed, som i den sag specialet analyserer, læner sig op af en mere absolut vurdering.

Derudover ses det også fra analysen af SRB-sagen, at EDPS også anvender den absolutte tilgang i deres vurdering af personoplysninger. De forsøger at gøre det gældende, at der bare skal være én, der har adgang til de supplerende oplysninger for, at oplysningerne kan kaldes personoplysninger.

Det kan på baggrund af specialets undersøgelsesområde dermed ses, at nogle tilsynsmyndigheder som Spaniens og EDPS støtter sig op af en vurdering, som EU-domstolen ikke er enig i, hvis man følger EU-domstolens retspraksis, som ses anvendt i dette speciale til besvarelse af problemformuleringen.

Denne uenighed om og forskel i fortolkning af personoplysningsbegrebet fra de forskellige tilsynsmyndigheder, og endda EU's egen tilsynsmyndighed, kan have store betydninger for de selskaber, der skal forsøge at følge reglerne under databeskyttelsesforordningen. Det kan umiddelbart anses for at være en hindring for et selskab, at udføre deres erhverv, hvis en del af erhvervet består i behandling af (person)oplysninger på tværs af landegrænser, idet selskabet ikke kan forvente, at kravene for eller vurderingen af personoplysninger er ens i de relevante områder. Et selskab der kommer frem til den konklusion, at de ikke kan identificere den registrerede og dermed mener, at de ikke behandler personoplysninger, kan pludseligt komme i klemme i situationer, hvor den relevante tilsynsmyndighed bruger den absolutte tilgang, da kravene og standarden herved er er lavere, for hvornår der er tale om personoplysninger.

Det kan også ses ud fra Omnibus-forslaget, at EU-kommissionen ønsker at præcisere dette område, og dermed forsøge at hjælpe de påvirkede, ved at give dem en tydeligere definition at gå efter. Forslaget vedtages dog muligvis ikke på baggrund af det tidligere nævnte læk.

EDPB og EDPS mente dog i sidste ende ikke, at ændringsforslaget var en god løsning. Det ville give for mange muligheder for visse selskaber til at prøve at komme uden om databeskyttelsesforordningen, og dermed svække beskyttelsen af borgerne.

EU er dannet for at beskytte EU-borgerne samt styrke den indre handel mellem medlemslandene. Det er dermed vigtigt, at begge disse aspekter bliver taget hånd om i alt EU-lovgivning. Problemet med at der er uenighed mellem tilsynsmyndighederne og EU-domstolens fortolkning er, at borgerne ikke ved, hvornår de bør være beskyttet af databeskyttelsesforordningen, og de dataansvarlige ved ikke, hvornår de er omfattet af forordningen og dets reguleringer, og hvornår de ikke er. De dataansvarlige kan dermed ende med at bruge flere ressourcer end nødvendigt på at overholde databeskyttelsesforordningen, eller slet ikke bruge de krævede ressourcer, da de mener, at de slet ikke behandler personoplysninger. Det er dermed vigtigt og relevant, at dette område bliver undersøgt til bunds og den korrekte vurderingsform bliver klarlagt f.eks. gennem en ændring i definitionen.

Konklusionen på dette speciale bygger på analyser af nogle udvalgte EU-domme og tilsynsmyndighedsafgørelser. Specialet har ud fra sin opbygning ikke haft mulighed for at indeholde alle relevante EU-domme eller tilsynsmyndighedsafgørelser. Der kan være tilsynsmyndighedens afgørelser fra andre tilsynsmyndigheder, der kan give et bedre og mere omfattende indblik i, hvordan hoveddelen af tilsynsmyndigheder fortolker identifikationskravet, og der kan være sager fra EU-domstolen, der giver et andet billede af hvilken vurderingsmetode, de anvender, hvis disse var medtaget. Der kan i fremtiden også komme sager fra EU-domstolen, hvor de vurderer anderledes på bestemte sager, hvorfor der ikke kan gives et entydigt svar på hvilken af disse vurderinger, der er den korrekte for alle sager.

Specialets analyse og konklusion kan være med til at skabe et bedre indblik i, hvordan EU-domstolen fortolker på dette område, samt give indblik i situationer, hvor dette problem kan anses for at være en væsentlig udfordring, der skal tages stilling til. Som nævnt har specialet sine begrænsninger i, at det er lavet på forholdsvis få sager, set ud fra den samlede mængde materiale herunder antal af tilsynsmyndigheder og deres afgørelser, samt domme der kan være relevante for området, som et senere speciale eller en større undersøgelse kan bringe med i dets vurdering af samme område.

12. Litteraturliste

12.1. Love og forordninger:

DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF

LISSABONTRAKTATEN OM ÆNDRING AF TRAKTATEN OM DEN EUROPÆISKE UNION OG TRAKTATEN OM OPRETTELSE AF DET EUROPÆISKE FÆLLESKAB (2007/C306/01)

Lov om behandling af personoplysninger, Lov nr 429 af 31/05/2000

12.2. Lovforslag

Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om ændring af forordning (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 og direktiv 2002/58/EF, (EU) 2022/2555 og (EU) 2022/2557 for så vidt angår forenkling af det digitale regelsæt og om ophævelse af forordning (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 og direktiv (EU) 2019/1024 (den digitale omnibus)

12.3. Domme

C-413/23 SRB v EDPS

C-434/16 Peter Nowak v Data Protection Commissioner

C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*

C-604/22 IAB Europe

Forslag til afgørelse generaladvokaten, Patrick Breyer v. Bundesrepublik Deutschland sag af 12 maj, 2016

12.4. Tilsynsmyndigheds afgørelser

2023-211-0004. Afsagt af den danske tilsynsmyndighed.

PS/00158/2022. Afsagt af den spanske tilsynsmyndighed.

SAN-2024-013. Afsagt af den franske tilsynsmyndighed.

12.5. Bøger:

Blume, P. (2020). *Persondatarettens kilder og metode* (1. udgave). København: Djøf Forlag.

Hamer, C. R., & Schamburg-Müller, Sten., (2020). *Juraens verden* (1. udgave). København: Djøf Forlag.

Hansen, L., & Werlauff, E. (2022). *Den juridiske metode - en introduktion* (3. udgave). København: Djøf Forlag.

Munk-Hansen, C. (2018). *Retsvidenskabsteori* (2. udgave). København: Djøf Forlag.

Nielsen, K. K., & Lotterup, A. (2025). *Databeskyttelsesforordningen og databeskyttelsesloven* (2. udgave). København: Djøf Forlag.

Udsen, H., & Knobel, D., (2026) *Introduktion til databeskyttelsesret* (1. udgave). www.Databeskyttelsesret.dk

12.6. Afhandlinger:

Andersen, K. B. H. (2025). *Personoplysningsbegrebet i GDPR.* Aalborg University Open Publishing. https://doi.org/10.54337/aau796580654

12.7. Udtalelser og rapporter:

EDPB-EDPS JOINT OPINION 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)

Justitsministeriets betænkning nr. 1565/2017

NOYB, Digital Omnibus - First Analysis of Select GDPR and ePrivacy Proposals by the Commission version 3.0. Lokaliseret på: https://noyb.eu/en/digital-omnibus-report-v3-analysis-select-gdpr-and-eprivacy-proposals-commission

Wp29's vejledning nr. 4/2007 af 20. juni 2007 om »begrebet personoplysninger«

12.8. Online dokumenter og hjemmesider:

CBS Library & Academic Services (u.d.) *Danske Retskilder: Retsafgørelser (retspraksis).* Lokaliseret 16. februar 2026 på: https://libguides.cbs.dk/c.php?g=417461&p=2845256

Datatilsynet (u.d.) *Afgørelser.* Lokaliseret d. 22. februar 2026 på: https://www.datatilsynet.dk/afgoerelser

Datatilsynet (u.d.) *Historien om databeskyttelse.* Lokaliseret d. 22. februar 2026 på: https://www.datatilsynet.dk/regler-og-vejledning/grundlaeggende-begreber#H1-gdpr

Den Europæiske Union (u.d.) *Sprog.* Lokaliseret d. 4. marts 2026 på: https://european-union.europa.eu/principles-countries-history/languages_da

Den Europæiske Unions Domstol (u.d) *Domstolen.* Lokaliseret d. 10. marts 2026 på: https://curia.europa.eu/site/jcms/d2_5093/da/domstolen

European Data Protection Board (u.d.) *Arv: Artikel 29-gruppen.* Lokaliseret d. 3. marts 2026 på: https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_da

European Data Protection Board (u.d.) *Role of the EDPB.* Lokaliseret 24. februar 2026 på: https://www.edpb.europa.eu/role-edpb_en

European Data Protection Supervisor (u.d.) *About us.* Lokaliseret 3. marts 2026 på: https://www.edps.europa.eu/about/about-us_en?etrans=da

Folketinget (u.d.) *EU's Love.* Lokaliseret d. 24. februar 2026 på: https://www.eu.dk/da/fakta-og-tal/s%C3%A5dan-lovgiver-eu/eus-love

Iapp (23.02.26) *EU member states' leaked Digital Omnibus compromise proposal eliminates revised GDPR definition of 'personal data'.* Lokaliseret på: https://iapp.org/news/a/eu-member-states-leaked-digital-omnibus-compromise-proposal-eliminates-revised-gdpr-definition-of-personal-data

Iapp (14.01.2026*) SRB pseudonymization case withdrawn from EU General Court.* Lokaliseret på: https://iapp.org/news/a/srb-pseudonymization-case-withdrawn-from-eu-general-court

JUC (u.d.) *Max Schrems.* Lokaliseret d. 16. april 2026 på: https://juc.dk/undervisere/max-schrems